08/2022

SECURITY MAGAZINE

Bezpieczeństwo | Technologia | Wiedza | Najlepsze standardy

Jak zabezpieczyć nieopłacone należności kontrahentów?

Nie tylko komputer może paść ofiarą hakerów

Background screening Wczesna linia obrony

Bezpieczeństwo podczas sezonów zakupowych

POST MORTEM, czyli co po cyberkryzysie?

SPIS TREŚCI

SZANOWNI PAŃSTWO,

to wydanie zdominowały relacje z wydarzeń związanych z bezpieczeństwem. Cieszy nas to szczególnie, bo przecież październik był Europejskim Miesiącem Cyberbezpieczeństwa. Jako patroni medialni aż czterech wydarzeń ubiegłego miesiąca poświęconych branży security włączyliśmy się do tej ważnej akcji jeszcze bardziej.

Zresztą już samo zakwalifikowanie przez NASK naszego wydania jako ogólnoeuropejską inicjatywę, która ma na celu edukować i uświadamiać Polaków, jak ważne jest cyberbezpieczeństwo, było dla nas wyzwaniem. Oprócz pracy nad miesięcznikiem przez cały październik w naszych social mediach zamieszczaliśmy grafiki, mające uświadamiać, z jakimi cyberzagrożeniami obecnie się mierzymy. Podsumowanie Europejskiego Miesiąca Cyberbezpieczeństwa autorstwa NASK opublikujemy w wydaniu grudniowym i zapewnimy, że będzie to interesująca lektura.

Równie ciekawie zapowiada się także nasze aktualne wydanie. Dużo w nim bardzo konkretnych podpowiedzi, co robić, by zabezpieczyć firmę przed oszustami, ale również kontrahentami, którzy zalegają z opłatami. Dowiecie się, jak przechytrzyć firmowe kryzysy, ale również co robić, kiedy już do cyberkryzysu dojdzie. Przed szałem zakupów polecamy też lekturę, na co uważać, by nie złapać się na hakerski haczyk, zarówno jako przedsiębiorca, jak i konsument.

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

JAK ZABEZPIECZYĆ NIEOPŁACONE NALEŻNOŚCI KONTRAHENTÓW?

Piotr Cholewczyński
INFINITY Brokerzy Ubezpieczeniowi

Ostatnie dwa lata, które przyniosły kryzys gospodarczy, energetyczny, czy przerwane łańcuchy dostaw, pokazały, jak trudno dziś utrzymać stabilny rozwój firmy. W jaki sposób zabezpieczyć się przed takim zagrożeniem? Co może dać przedsiębiorstwu ubezpieczenie należności handlowych?

„CZARNE ŁABĘDZIE”

Poniższy termin jest stosowany w ekonomii i oznacza nieoczekiwane zdarzenie, którego przewidzenie jest praktycznie niemożliwe. Zjawiska tego rodzaju mają najczęściej negatywny wpływ na naszą gospodarkę i charakteryzują się brakiem możliwości ich przeczucia w oparciu o wcześniejsze dane historyczne i doświadczenia.

Ostatnie wydarzenia związane z wojną w Ukrainie, epidemią Covid-19, a w konsekwencji przerwanymi łańcuchami dostaw, kryzysem energetycznym itp. powodują, że możemy śmiało założyć, iż żyjemy obecnie w czasach „czarnych łabędzi”.

W obecnej sytuacji geopolitycznej, terminowe spływanie należności od kontrahentów staje się szczególnie ważne w utrzymaniu stabilnego rozwoju firmy. Prowadzenie biznesu staje się coraz bardziej ryzykownym przedsięwzięciem. Coraz częstszym problemem okazują się opóźnienia w regulowaniu należności.

Niewypłacalność odbiorcy, może negatywnie wpływać na płynność przedsiębiorstwa, a tym samym na możliwość regulowania własnych zobowiązań. Ryzyko sprzedaży z odroczonym terminem płatności możemy zabezpieczyć poprzez wybór ubezpieczenia należności handlowych.

Wzrost liczby orzeczeń o niewypłacalności w roku 2022 w porównaniu do roku 2021 to aż 10%.

Jak zabezpieczyć nieopłacone należności kontrahentów?

KTO OFERUJE UBEZPIECZENIA NALEŻNOŚCI HANDLOWYCH?

Na naszym rynku ubezpieczenie należności oferowane jest przez kilku ubezpieczycieli:

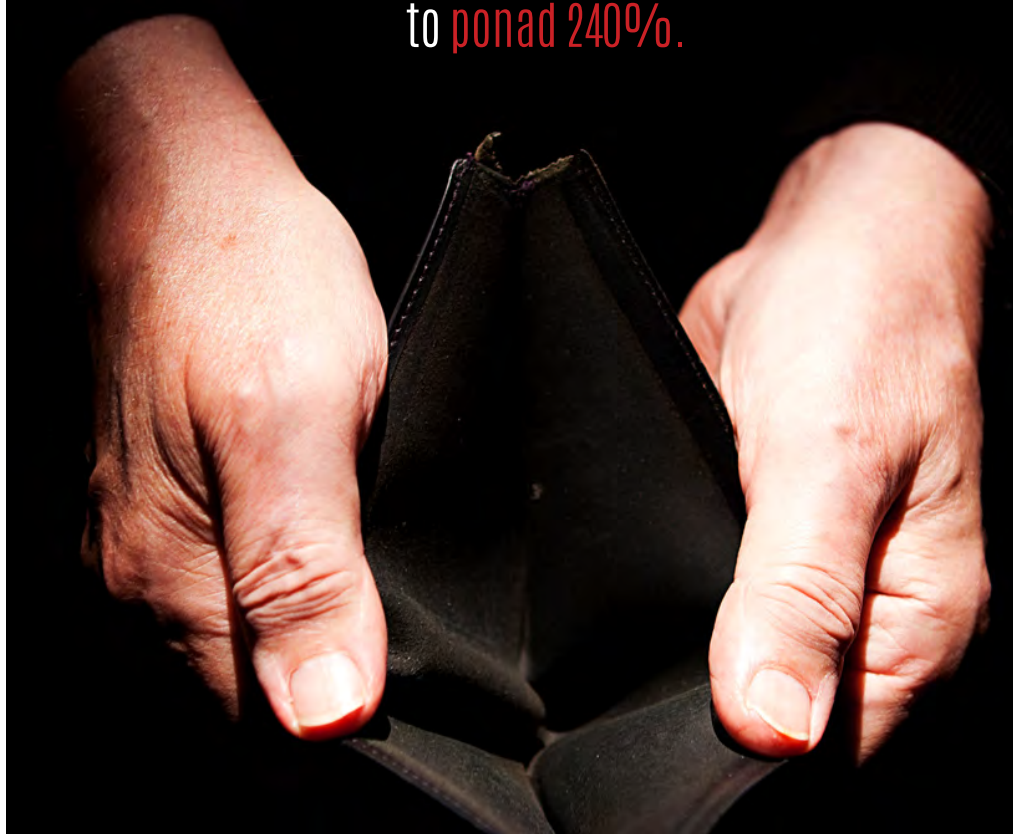
- Atradius Crédito y Caución S.A. de Seguros y Reaseguros Spółka Akcyjna Oddział w Polsce
- Compagnie Francaise D'assurance Pour Le Commerce Exterieur Sa Oddział w Polsce (Coface Poland)
- Towarzystwo Ubezpieczeń Euler Hermes SA (obecnie Allianz Trade)
- Korporacja Ubezpieczeń Kredytów Eksportowych S.A. (KUKE)
- Credendo - Excess & Surety Spółka Akcyjna Oddział w Polsce
- Powszechny Zakład Ubezpieczeń Spółka Akcyjna (PZU)
- Sopockie Towarzystwo Ubezpieczeń ERGO Hestia S.A.

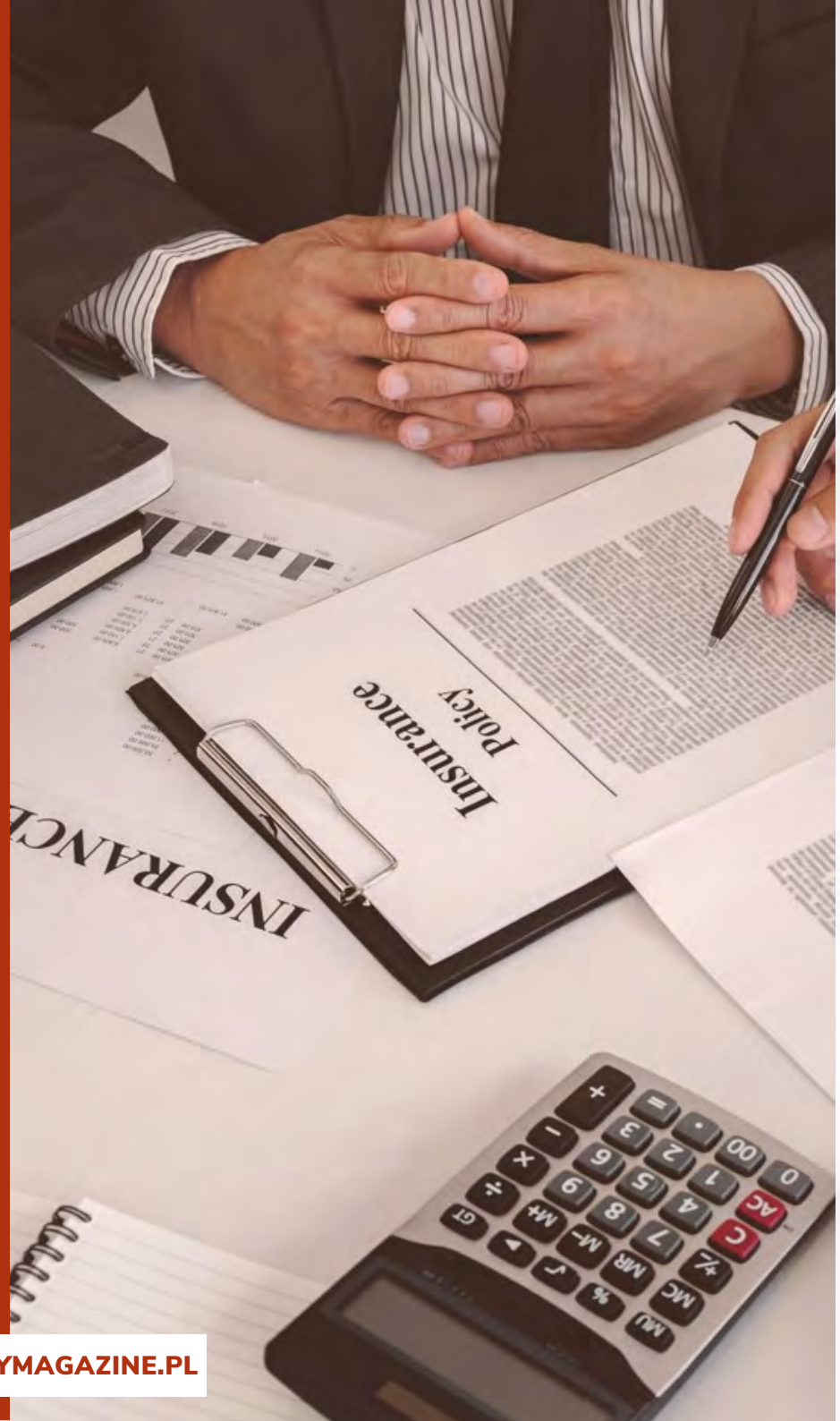
CO ZAPEWNIA UBEZPIECZENIE NALEŻNOŚCI HANDLOWYCH?

Ubezpieczenie należności handlowych polega na zapewnieniu ochrony w związku z nieopłaceniem przez odbiorców wystawionych faktur za sprzedane towary lub wykonane usługi.

W porównaniu do roku 2010 liczba orzeczeń o niewypłacalności polskich spółek zwiększyła się o:
- 40% w roku 2019
- 80% w roku 2020
- 210% w roku 2021

Przewidywany wzrost niewypłacalności w roku 2022 w porównaniu do roku 2010 to ponad 240%.





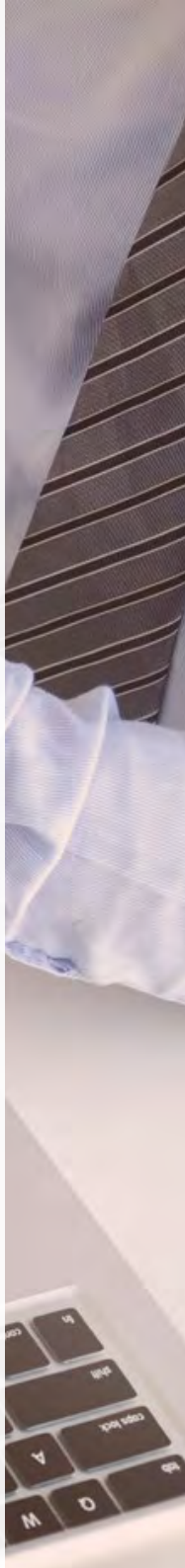
Posiadanie ubezpieczenia należności nie gwarantuje automatycznej zapłaty należności przez ubezpieczyciela w terminie płatności wskazanym na fakturze - nie należy porównywać tego rozwiązania do faktoringu, który jest zazwyczaj znacznie droższym rozwiązaniem.

Ochrona ubezpieczeniowa obejmuje ryzyko braku zapłaty bezspornych i wymagalnych należności w sytuacji braku jej uregulowania w określonym w umowie terminie (standardowo 120-180 dni, zdarzają się również okresy krótsze 60-90 dni). Odszkodowanie będzie należne również w przypadku trwałej niewypłacalności kontrahenta (prawnej niewypłacalności).

WARTOŚCI DODANE POSIADANIA UBEZPIECZENIA NALEŻNOŚCI HANDLOWYCH

Wsparcie ubezpieczyciela w procesie windykacji

W przypadku braku uregulowania należności ubezpieczyciel może przejąć kwestie windykacji. Okres prowadzenia windykacji zależy od oferty/ubezpieczyciela i wynosi zazwyczaj od 60 do 180 dni. W przypadku braku skutecznej windykacji we wskazanym terminie ubezpieczyciel przystępuje do wypłaty odszkodowania za niezapłaconą należność. Wypłacone odszkodowanie jest pomniejszone o udział własny, który wynosi najczęściej 10% wysokości należności.



Wsparcie w windykacji jest szczególnie istotne w przypadku obsługi klientów zagranicznych, gdzie możemy spotkać się z wieloma problemami:

- koszt prowadzenia procedury windykacyjnej przez spółkę (za pośrednictwem zagranicznych specjalistów w zakresie windykacji) może okazać się bardzo wysoki.
- różnorodność przepisów w zakresie windykacji w zależności od kraju, z którego pochodzi kontrahent.
- czas prowadzenia procedury windykacyjnej może okazać się zbyt długi, aby zapewnić spółce odpowiednią płynność finansową.

Z uwagi na to, że większość z ubezpieczycieli specjalizujących się w ubezpieczaniu należności handlowych działa globalnie, są w stanie przeprowadzić skuteczną i sprawną windykację nawet w przypadku kontrahentów „z drugiego końca świata".

Narzędzia IT dostarczane przez ubezpieczyciela wspomagające zarządzanie należnościami

Część ze wskazanych powyżej ubezpieczycieli udostępnia klientom specjalistyczne narzędzia IT za pomocą których możliwe jest, m.in.:

- zweryfikowanie aktualnego stanu płynności finansowej kontrahentów,
- stałe monitowanie kondycji finansowej kontrahentów,
- bieżące administrowanie wysokością limitów należności handlowych dla poszczególnych kontrahentów (optymalizuje to koszt ubezpieczenia),

Wzrost liczby orzeczeń o niewypłacalności w Europie Zachodniej:

- 19% w roku 2020
+ 6% w roku 2021
+ 14 % w roku 2022 (prognoza)
+ 14% w roku 2023 (prognoza).

Wiele firm będzie borykało się ze spadkiem kluczowych wskaźników kondycji finansowej, co finalnie wpłynie na zatory płatnicze oraz wzrost liczby upadłości.

- monitorowanie całego procesu windykacji - klient przez system posiada stały podgląd na bieżący stan windykacji,
- monitowanie procedury wypłaty należności w przypadku braku skutecznej windykacji lub częściowego odzyskania należności.

KOSZT UBEZPIECZENIA

Na koszt ubezpieczenia wpływa głównie wysokość obrotu z kontraktów przyjętych do ubezpieczenia. Drugim istotnym czynnikiem wpływają-cym na wysokość stawek w ubezpieczeniu jest rodzaj działalności wykonywanej przez ubezpieczonego.

Ubezpieczyciele opierają się najczęściej na PKD zarejestrowanych spółek. Na wycenę ma wpływ również historia szkodowa podmiotu występującego o ofertę oraz ponoszone straty z tytułu braku uregulowanych należności. Stawki za ubezpieczenie wahają się zazwyczaj od 0,1% do około 1% wartości ubezpieczonych obrotów.

Przykładowo, spółka z branży technologicznej wykonująca usługi dla kontrahentów z całego świata działających w różnych branżach może liczyć na **następujące składki w zależności od wysokości rocznego obrotu przyjętego do ubezpieczenia:**

- obrót 3 mln zł – składka 16 200 zł
- obrót 5 mln zł – składka 22 500 zł
- obrót 10 mln zł – składka 30 000 zł
- obrót 26 mln zł – składka 62 400 zł
- obrót 40 mln zł – składka 72 000 zł
- obrót 150 mln zł – składka 195 000 zł.

PROCEDURA ZAWARCIA UBEZPIECZENIA

Procedura zawarcia ubezpieczenia należności jest dość prosta. Można ją podzielić na dwa etapy.

Pierwszy z nich ma na celu ustalenie warunków ubezpieczenia (stawek).

Drugi jest związany jest z ustalaniem przez ubezpieczyciela limitów ochrony dla kontrahentów. Im lepsza kondycja finansowa kontrahenta, tym możliwy wyższy limit należności do uzyskania.

Informacje, których wymaga ubezpieczyciel we wniosku to, m.in.:

- struktura klientów (najwięksi odbiorcy pod względem realizowanego obrotu przyjętego do ubezpieczenia),
- warunki płatności oferowane klientom,
- struktura obrotów i wyniki firmy,
- straty z tytułu niezapłaconych należności

- w ostatnich 2-3 latach obrotowych i w bieżącym roku obrotowym,
- suma należności przeterminowanych w poszczególnych okresach kredytowania.

CO DAJE UBEZPIECZENIE NALEŻNOŚCI HANDLOWYCH?

Płynność finansowa

Umożliwia rozwój sprzedaży bez obaw o brak gotówki spowodowany nieopłacaniem faktur, ponieważ w sytuacji braku uregulowania należności lub niewypłacalności kontrahenta ubezpieczyciel pokryje należne bezsporne zaległości.

Wzrost konkurencyjności

Wydłużenie terminów płatności umożliwia zaoferowanie odbiorcom usług bardziej konkurencyjnych warunków współpracy i dzięki temu zwiększa szansę na pozyskanie wartościowego kontraktu.

Ułatwienie podejmowania decyzji

Większość ubezpieczycieli udostępnia specjalistyczne narzędzia do monitorowania sytuacji finansowej kontrahenta, co ogranicza ryzyko przy podpisywaniu nowych umów. Dzięki temu możliwe jest skoncentrowanie się na podstawowej działalności przedsiębiorstwa oraz jego celach strategicznych.

Wsparcie przy windykacji należności

Ubezpieczyciel przejmuje czynności i koszty związane z odzyskaniem należności, co oszczędza czas i daje możliwość ograniczenia wydatków.

Lepszy dostęp do finansowania

Ubezpieczenie podnosi wiarygodność firmy wobec banków i firm faktoringowych, dając szansę wynegocjowania lepszych warunków współpracy i uzyskania dodatkowych źródeł finansowania działalności przedsiębiorstwa.

PODSUMOWANIE

Ubezpieczenie należności handlowych jest skutecznym rozwiązaniem „czarnych łabędzi". Jest warte uwagi w przypadku współpracy z rynkami zagranicznymi, na których od 2 lat panuje wzrost liczby niewypłacalnych spółek, a prognozy wskazują na pogłębianie się tego problemu. Korzystnym rozwiązaniem jest możliwość wyboru zabezpieczenia się przed nieopłaconymi należnościami poszczególnych kontrahentów bez obejmowania całego obrotu spółki. Pozwala to na optymalizację kosztu ubezpieczenia skupiając się wyłącznie na ubezpieczeniu najbardziej ryzykownego biznesu. Jednocześnie jest to bardzo korzystne narzędzie wspomagające w istotny i aktywny sposób zarządzanie należnościami w spółce.

PATRONAT
SECURITY MAGAZINE

ADVANCED THREAT SUMMIT 2022

Zero Day on every day czyli nie znacie dnia i godziny - to temat przewodni Advanced Threat Summit 2022 – jednej z najważniejszych i najciekawszych konferencji dla managerów cyberbezpieczeństwa.
W tym roku spotykamy się już po raz dziewiąty 22-24 listopada, w formule hybrydowej: on-site — bezpośrednio w sali konferencyjnej hotelu Marriott w Warszawie oraz na wieczornych spotkaniach networkingowych, a dla zainteresowanych również online.

Program konferencji jest odpowiedzią na potrzeby i zainteresowania profesjonalistów z branży cyberbezpieczeństwa, którzy czuwają nad bezpieczeństwem cyfrowym i informacyjnym swoich organizacji.
Nikt odpowiedzialnie nie może stwierdzić, że jego organizacja jest w pełni bezpieczna. Nieoczekiwane zjawiska czy zagrożenia Zero Day mogą zmaterializować się w każdej chwili. Można za to zrobić wiele, by nasza organizacja była przygotowana, aby na te niespodziewane zdarzenia odpowiednio zareagować i ochronić ciągłość funkcjonowania biznesu. O tym chcemy rozmawiać podczas tegorocznego ATS-u.
Advanced Threat Summit to niezmiennie wyjątkowi goście specjalni oraz reprezentacja znakomitych ekspertów!

Rezerwujcie bilety już dziś!
Z kodem promocyjnym
SECURITYMAGAZYN10
otrzymacie 10% rabatu!

Szczegóły na stronie wydarzenia.

SECURITYMAGAZINE.PL

CYBER-BEZPIECZEŃSTWO NIE BYŁO BARDZIEJ ISTOTNE NIŻ DZIŚ. CYBER24 DAY

PATRONAT
SECURITY MAGAZINE

Fot. Robert Suchy (grupa Defence24)

Temat bezpieczeństwa cyfrowego stał się jeszcze bardziej gorący od 24 lutego tego roku. Choć wojna w cyberprzestrzeni rozpoczęła się wcześniej, to militarny atak na Ukrainę zmusił władze, służby i obywateli do baczniejszego obserwowania manewrów hakerskich i szerokiego działnia w zakresie cyberbezpieczeństwa.

Fot. Robert Suchy (grupa Defence24)

PO RAZ DRUGI

Grupa Defence24 zorganizowała po raz kolejny konferencję Cyber24 Day, która odbyła się w Warszawie.

- *Rozmawialiśmy o najważniejszych zagadnieniach dotyczących cyberbezpieczeństwa, nowoczesnych technologii, cyberedukacji, sztucznej inteligencji czy komunikacji strategicznej* - zaznaczają organizatorzy jednego z najważniejszych wydarzeń w Polsce poświęconych bezpieczeństwu.

12 października dyskutowano m.in. o hakerach i ich znaczeniu o Big Data jako następnej domenie walki, o tym, jak SI może przeciwdziałać terroryzmowi, o edukacji żołnierzy i społeczeństwa w obronie kraju, o infrastrukturze krytycznej w dobie cyberzagrożeń, o komunikacji strategicznej, o rozwiązaniach technologii chmurowej, a także o kobietach w branży cyberbezpieczeństwa.

Lista tematów była bardzo długa, a co za tym idzie, grono prelegentów i ekspertów było szerokie. Na Cyber24 Day zaproszeni byli m.in.:

- **Janusz Cieszyński,** Sekretarz Stanu i Pełnomocnik ds. Cyberbezpieczeństwa w Kancelarii Prezesa Rady Ministrów,
- **Michał Wiśniewski**, Podsekretarz Stanu w Ministerstwie Obrony Narodowej, Pełnomocnik MON ds. bezpieczeństwa cyberprzestrzeni,

Fot. Robert Suchy (grupa Defence24) (2)

- **Paweł Lewandowski**, Podsekretarz Stanu w Kancelarii Prezesa Rady Ministrów,
- **Kamil Basaj**, Rządowe Centrum Bezpieczeństwa,
- **nadinsp. Adam Cieślak**, Komendant Centralnego Biura Zwalczania Cyberprzestępczości,
- **Andrzej Dulka**, Prezes Polskiej Izby Informatyki i Telekomunikacji,
- **Krzysztof Bosak**, Poseł na Sejm; Konfederacja Wolność i Niepodległość,
- **Nikodem Bończa Tomaszewski**, Prezes Zarządu EXATEL S.A.,
- **Krzysztof Dyki**, Prezes ComCERT S.A., Grupa Asseco,
- **płk rez. Paweł Dziuba,** Dyrektor Eksperckiego Centrum Szkolenia Cyberbezpieczeństwa,
- **dr Krzysztof Gawkowski**, Poseł na Sejm, Członek Komisji Cyfryzacji, Innowacyjności i Nowoczesnych Technologii; Nowa Lewica,
- **Adam Dzwonkowski**, Dyrektor ds. technologii wspierających sektor wojskowy, Microsoft,
- **prof. Marco Lombardi**, profesor Università Catolica del Sacro Cuore z Mediolanu, Dyrektor Centrum Badań ITSTIME,
- **płk. dr inż. Rafał Kasprzyk**, Zastępca Dziekana Wydziału Cybernetyki, Wojskowa Akademia Techniczna,
- **Sebastian Kondraszuk,** Kierownik Działu CERT Polska w NASK-PIB.

CYBERBEZPIECZEŃSTWO WAŻNE JAK NIGDY DOTĄD

- Cyberataki są obecnie zjawiskiem powszechnym. Zamiast zarządzać kryzysami tworzonymi przez nowe technologie, chcemy przewidywać nowe zagrożenia i być o krok przed cyberprzestępcami. W ostatnim roku co trzecia firma zmierzyła się z naruszeniem cyberbezpieczeństwa swoich systemów.

Fot. Robert Suchy (grupa Defence24) (2

Fot. Robert Suchy (grupa Defence24) (3)

Fot. Robert Suchy (grupa Defence24) (2)

Najczęstszym zagrożeniem jest szkodliwe oprogramowanie, w tym ransomware oraz klasyczne ataki sieciowe na infrastrukturę firmy. Firmy w celu ochrony sięgają do szeregu rozwiązań technologicznych. Rosnąca skala cyberzagrożeń, trend pracy zdalnej, sieć 5G coraz częstsze wykorzystywania IoT oraz przyspieszająca transformacja wymuszają na firmach zainteresowanie w kierunku cyberbezpieczeństwa - podkreślił August Żywczyk, Członek Zarządu Defence24.

Janusz Cieszyński, Pełnomocnik rządu ds. cyberbezpieczeństwa w KPRM, zaznaczył, że bardzo istotne jest to, by w obszarze cyberbezpieczeństwa, cyberprzestrzeni - współpracować w realny sposób. - *Po pierwsze, być w stanie otworzyć się na zewnętrzne podmioty, z firmami, ale jest to też praca w ramach rządu. Jest wiele instytucji, które na poziomie krajowym odpowiadają za ten obszar, ale też wiemy, że system jest tak skonstruowany, że nawet, jeśli te instytucje działałyby wspaniale, to jeżeli nie będą dobrze działały zespoły, to też na nic się nie zda* - powiedział, dodając, że w tym roku było kilka takich momentów, gdzie reakcja była bardzo szybka i adekwatna do trudnej sytuacji, w której się znaleźliśmy.

WOJNA W CYBERPRZESTRZENI TRWA CAŁY CZAS

Przy okazji zapowiedział, że projekt nowelizacji ustawy o **Krajowym Systemie Cyberbezpieczeństwa** trafił do Komitetu Rady Ministrów ds. Bezpieczeństwa Narodowego i Spraw Obronnych.

- *Najważniejsze zmiany w nowelizacji ustawy dotyczą powołania Funduszu Cyberbezpieczeństwa, wprowadzenie jednolitej siatki wynagrodzeń dla ekspertów zajmujących się cyberbezpieczeństwem w instytucjach publicznych. To oczekiwana, ważna zmiana. Oprócz tego chcemy wyjaśnić kwestie związane*

Fot. Robert Suchy (grupa Defence24) (4)

z operatorem bezpieczeństwa sieci 5G. Wiemy, że momorandum w tej sprawie było podpisane już dwa lata temu. Bardzo dużo udało się zrobić, ale wciąż jest jeszcze kwestia pewnych ustaleń - tak, aby ten projekt mógł ruszyć - skomentował w rozmowie z organizatorem konferencji Janusz Cieszyński. Dodał, że w ramach Funduszu Cyberbezpieczeństwa będą realizowane inwestycje w jednostkach, które odpowiadają za cyberbezpieczeństwo w Polsce. - NASK, służby, policja, każdy będzie mógł o te środki wystąpić. Siłą rzeczy to tematy, które lubią ciszę i o szczegółach będziemy mogli mówić wtedy, kiedy będą zrealizowane konkretne inwestycje - zadeklarował.

CO DECYDUJE O CYBERKONFLIKCIE?

- Istnieją trzy kategorie czynników, które mogą zadecydować o przyszłym cyberkonflikcie. To technologia, rozwój i ludzie oraz partnerstwo. Powinniśmy uczyć się na naszych błędach, ale i na błędach naszych partnerów, wyciągać wnioski i iść do przodu - powiedział gen. bryg. Karol Molenda, Szef Narodowego Centrum Bezpieczeństwa Cyberprzestrzeni.

- Mamy 4,6 miliarda użytkowników internetu. W tej liczbie mamy 4,2 miliardy użytkowników mediów społecznościowych. Na naszym podwórku, na 37 milionów obywateli mamy 32 miliony użytkowników sieci internet i prawie 27 milionów użytkowników portali społecznościowych - zaznaczył Molenda. To dane, wobec których nie można przejść obojętnie.

TYLKO RAZEM

- Cyberbezpieczeństwo to gra zespołowa. To proces, który angażuje bardzo wielu interesariuszy - od administracji rządowej wysokiego szczebla, aż po każdego z nas. Wszyscy razem, i podmiot prywatny, i globalny dostawca, i mała firma, i administracja lokalna – wszyscy razem pracujemy na to, żeby zbudować naszą odporność na trudne czasy, które teraz nastały - podsumował Krzysztof Malesa, Dyrektor ds. strategii bezpieczeństwa Microsoft.

Patronat Security Magazine. Cyber24 Day

OBSŁUGA PRAWNA E-COMMERCE

WWW.RZETELNYREGULAMIN.PL

BEZPIECZEŃSTWO PODCZAS SEZONÓW ZAKUPOWYCH

Maciej Pawlak
Tpay

Black Friday i święta Bożego Narodzenia to dla konsumentów czas wzmożonych zakupów, a dla sprzedawców – wytężonej pracy. Nie próżnują także... cyberprzestępcy. Co zrobić, aby nie dać się oszukać? Upolować superofertę, zamiast zostać upolowanym?

SPRZEDAWCO, BĄDŹ PRZYGOTOWANY!

Przed wprowadzeniem akcji sprzedażowych, sprzedawcy zazwyczaj zwracają uwagę m.in. na działania marketingowe, związane z SEM i SEO czy odpowiednie zatowarowanie. Choć aktywności te są ważne i bez wątpienia mogą pomóc w zapewnieniu właścicielom e-commerce zamówień, a konsumentom komfortu zakupów, to absolutnie priorytetowym zadaniem dla każdego sprzedawcy powinno być (nie tylko we wzmożonych okresach promocji) zadbanie o bezpieczeństwo – zarówno sklepu, jak i klientów. Jak się do tego przygotować?

Działanie z wyprzedzeniem

Niemalże z każdym rokiem gorączka przedświątecznych zakupów dopada sklepy coraz wcześniej. I choć w tym roku, ze strony konsumentów szał zakupowy może być nieco mniejszy, warto, aby sprzedawcy z dużym wyprzedzeniem przygotowali się pod względem wydajności wszelkich procesów. Tak, aby m.in. odpowiednio oszacowana liczba zamówień pozwoliła na płynną działalność biznesową.

Na straży stabilnej infrastruktury

Warto sprawdzić, czy systemy IT są gotowe pod względem wydajności - czy bez problemu obsłużą wzmożony ruch na stronie www. Należy także zweryfikować jak działają systemy zajmujące się automatyzacją i zoptymalizować działanie strony internetowej.

Trzeba również pamiętać o regularnej aktualizacji systemów IT pod kątem zabezpieczeń – tak, aby prosty incydent bezpieczeństwa nie przeszkodził w obsłudze „gorącego" okresu zakupowego. Wciąż najczęstszym modelem ataku jest **ransomware**, czyli kategoria złośliwego oprogramowania, które szyfruje pliki lub urządzenie użytkownika, następnie żąda anonimowej płatności (okupu) w celu przywrócenia dostępu. Aktualizacja systemów IT oraz wdrożenie dobrych programów antywirusowych to zatem prawdziwy „must have". Należy również rozważyć wykonywanie regularnych testów bezpieczeństwa systemów. Bardzo ważne jest ciągłe podnoszenie świadomości oraz edukacja pracowników w zakresie potencjalnych incydentów bezpieczeństwa.

Współpraca z zaufanym operatorem płatności

Aby prowadzić działalność i uruchomić e-płatności, właściciele e-commerce'ów muszą spełnić szereg wymogów.

Rozpoznawalna marka operatora to jednak nie wszystko – patrzmy na certyfikaty potwierdzające wiarygodność operatora i pozwalające im zapewnić odpowiedni poziom ochrony. Jednym z nich jest PCI DSS (Payment Card Industry Data Security Standard), będący potwierdzeniem spełniania norm wymaganych przez instytucje płatnicze do dostarczania płatności kartami. To pomoże utrzymać poufne dane w bezpiecznym „miejscu".

Nieuczciwi kupujący

Nie tylko konsument może zostać oszukany – może się to zdarzyć także sprzedawcom, którzy trafią na nieuczciwych kupujących.

Jedną z nadrzędnych kwestii, na którą sprzedający muszą zwrócić uwagę, jest wysyłka zamówionego towaru dopiero po opłaceniu (i zaksięgowaniu!) zamówienia przez klienta. Zdarza się bowiem, że klienci-oszuści proszą o natychmiastową wysyłkę bez potwierdzenia płatności. Przed takim incydentem może ochronić m.in. współpraca z operatorem płatności, zapewniającym sprzedawcy panel transakcyjny.

KONSUMENCIE – BĄDŹ CZUJNY!

Choć, jak wynika z badania na zlecenie Tpay, dla blisko 90% Polaków bardzo ważne jest bezpieczeństwo transakcji podczas e-zakupów, to respondenci zapytani o obawy związane z zakupami online, najczęściej wskazują na niezgodność towaru z oczekiwaniem (54 proc.), a dopiero później – na bezpieczeństwo swoich danych i własnego konta bankowego (49 proc.). Na co, kupując online, powinien zwrócić uwagę konsument, by pozostać bezpiecznym?

Warto pamiętać, że operatorzy płatności powinni być nadzorowani przez Komisję Nadzoru Finansowego i posiadać stosowną licencję na świadczenie usługi płatniczej (czy tak jest - można potwierdzić na stronie Komisji Nadzoru Finansowego).

Warto też sprawdzać listę ostrzeżeń publicznych KNF czy firma, z usług której chcemy skorzystać, nie została na niej przez regulatora umieszczona. Taka przezorność może nas w przyszłości uchronić od niejednej nieprzyjemności.

Fałszywe sklepy i promocje

Duże obniżki cenowe kuszą każdego, tym bardziej, jeśli od dawna polujemy na dany produkt. Przed kliknięciem w np. „Kupuję i płacę" , powinniśmy jednak zadać sobie pytanie: czy aż tak duża promocja, np. na najnowszy model smartfona, jest w ogóle możliwa? Niska, atrakcyjna cena to jedno, ale jest jeszcze jedna ważna kwestia do sprawdzenia – wiarygodność sklepu, który tak atrakcyjną cenę oferuje. Zanim damy się skusić na zamówienie dosłownie „za grosze", dokonajmy solidnego researchu. Sprawdźmy, jak długo e-sklep funkcjonuje na rynku, jakie ma opinie w sieci (najlepiej w niezależnych serwisach oceniających sklepy internetowe) oraz czy na jego stronie www znajdziemy regulamin zakupów i informacje na temat sprzedawcy – pełną nazwę, siedzibę i dane kontaktowe. Istotne będą także informacje dotyczące obsługi klienta: terminy dostaw oraz polityka zwrotów.

Uwaga na dropshipping

W okresie przedświątecznym nasila się także skala oszustów korzystających z modelu dropshippingu, czyli takiego rodzaju sprzedaży, w którym produkty wystawione przez sprzedawcę w jego sklepie są wysyłane do klienta bezpośrednio od zewnętrznego dostawcy.

Co ważne, nawet jeśli natrafimy na uczciwych przedsiębiorców, działających w takim modelu, musimy pamiętać, że w przypadku problemów chociażby z wysyłką lub wadliwym towarem, możemy napotkać na problemy z wyegzekwowaniem reklamacji, którą de facto będziemy składać w kraju, z którego towar do nas dotarł (najczęściej są to kraje Azji). Oczekując na przesyłkę wysłaną w takim modelu trzeba także uzbroić się w cierpliwość - dostawa może zająć nawet kilka tygodni.

Wyłudzenia BLIK

Według wyników badania Tpay, spadł – choć nieznacznie (71%. vs. 70%) – odsetek osób, które preferują BLIKA spośród dostępnych płatności online. Ta metoda płatności ma jednak nie tylko swoje blaski, ale też cienie – stała się często wykorzystywana w oszustwach. Metoda „na BLIKA" polega na tym, że oszust, przejmując należący do kogoś profil w mediach społecznościowych, kontaktuje się ze znajomymi osoby, której profil p rzejął, prosząc ich o wsparcie finansowe (uzasadnione nagłą, wyjątkową sytuacją) i podanie kodu do płatności mobilnych (BLIK). Działalność przestępcza polega więc na wykorzystaniu zaufania. Skuteczną obroną przed takim atakiem jest nasza czujność – bądźmy uważni i asertywnie odmawiajmy „pomocy".

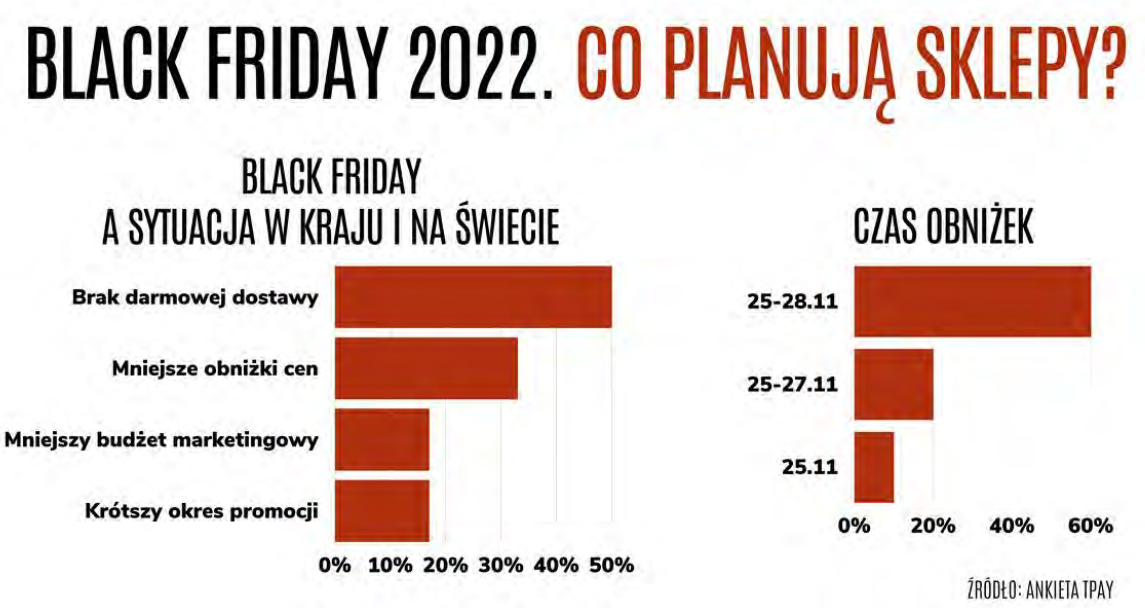
OFIARA „NA HACZYK"

Innym popularnym mechanizmem oszustwa jest klasyczny phishing. Obecnie jesteśmy świadkami coraz większej liczby tego typu oszukańczych kampanii oraz ich wyrafinowania. Nie muszą to być już tylko wiadomości e-mail, ale również sms. W okresie promocji i zakupów przedświątecznych skala takich kampanii na pewno wzrośnie. Możemy sobie wyobrazić scenariusz, gdy konsument otrzymuje np. maila z oszukańczego sklepu internetowego z bardzo atrakcyjną ofertą produktową.

Dając się nabrać i klikając w link zawarty w mailu – zostaniemy przekierowani do fałszywego sklepu, a następ-nie na stronę płatności i bankowości, aby wyłudzić nasze dane dostępowe a następnie wyprowadzić środki.

Mimo że wektor ataku jest w tym przypadku inny, to tego typu oszustwo może być bardzo trudne do wykrycia. Pamiętajmy, aby nie klikać w podejrzane linki i uważnie czytać otrzymywane wiadomości.

Zwracajmy uwagę, jaką dokładnie transakcję czy operację bankową autoryzujemy. Sprawdzajmy, czy w nazwie domeny nie ma literówek oraz czy przekierowanie do banku jest prawdziwe.

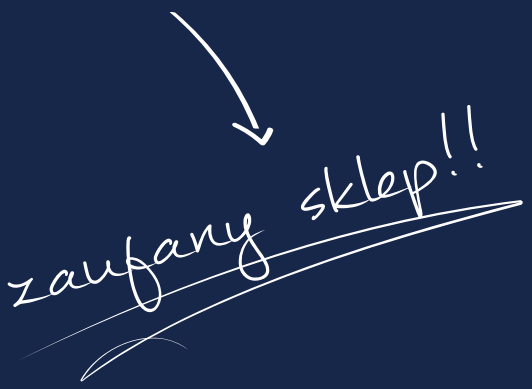


W przypadku wykrycia włamania, o incydencie niezwłocznie poinformujmy osobę, na której konto dokonano włamania.

Dokonajmy tego jednak innym kanałem komunikacji, niż ten, z którego być może doszło do oszustwa - najlepiej poprzez kontakt telefoniczny.

Taka osoba powinna w trybie pilnym zmienić swoje hasła dostępowe - tym bardziej, jeśli miała takie samo hasło do innych serwisów.

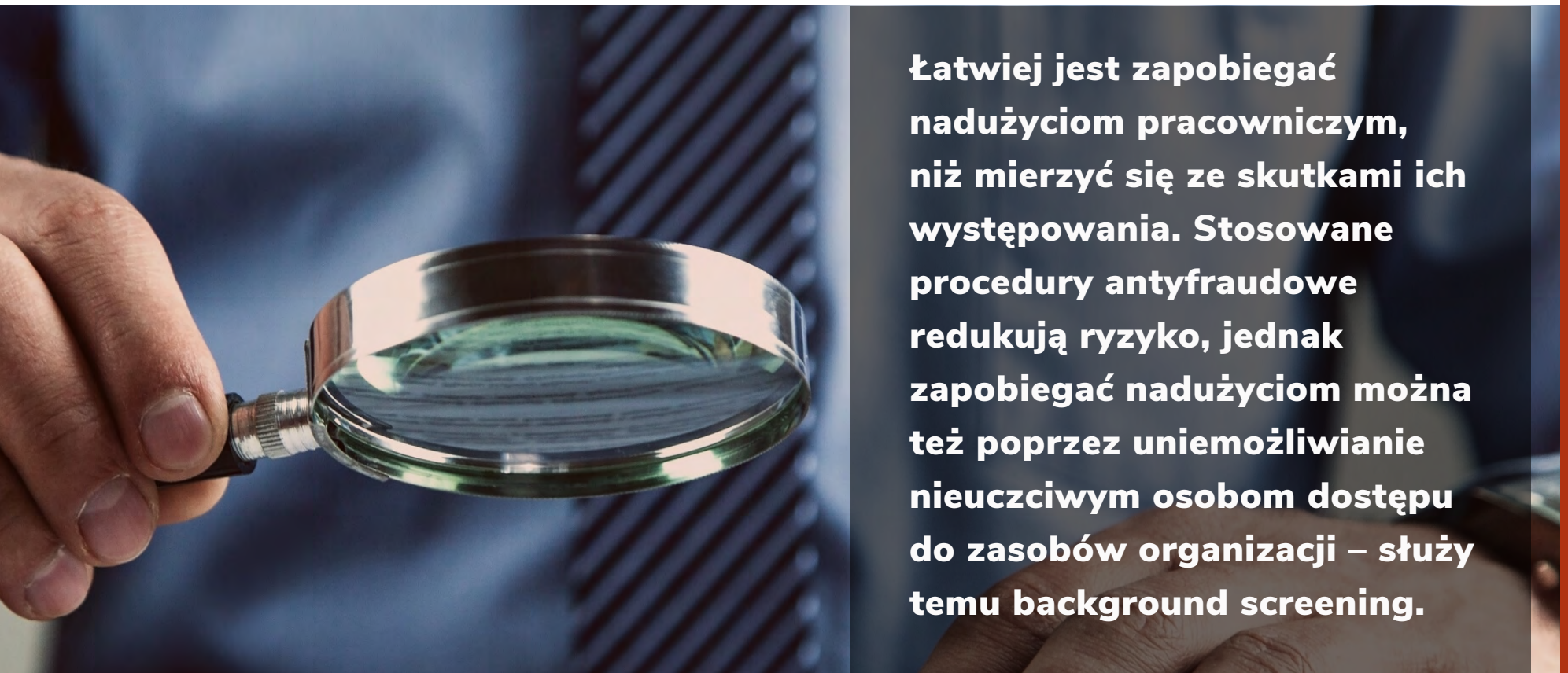
tpay zaufane płatności



www.tpay.com

BACKGROUND SCREENING – WCZESNA LINIA OBRONY

Rafał Lachowicz



Łatwiej jest zapobiegać nadużyciom pracowniczym, niż mierzyć się ze skutkami ich występowania. Stosowane procedury antyfraudowe redukują ryzyko, jednak zapobiegać nadużyciom można też poprzez uniemożliwianie nieuczciwym osobom dostępu do zasobów organizacji – służy temu background screening.

Nadużycia pracownicze to problem nie tylko powszechny, ale i kosztowny. Jak wskazują prowadzone w tym kierunku badania, ich ofiarą pada nawet co druga organizacja, bez względu na profil prowadzonej przez nią działalności. Przeciętna strata organizacji związana z wystąpieniem nadużyć to średnio 5% jej rocznych przychodów. Ale koszty finansowe to nie wszystko – nadużycia generują również poważne szkody wizerunkowe, fatalnie wpływają na reputację organizacji i osłabiają jej relacje biznesowe.

Istnieją mechanizmy kontrolne, które znacznie ograniczają ryzyko działania nieuczciwego pracownika na szkodę pracodawcy i wiele organizacji z powodzeniem je implementuje, nadużyciom pracowniczym można jednak przeciwdziałać już na etapie rekrutacji, a to poprzez background screening - staranną weryfikację wiarygodności kandydata oraz informacji przedstawianych w składanych przez niego dokumentach aplikacyjnych.

KŁAMSTWA W CV

Jak wykazało badanie przeprowadzone przez brytyjską Risk Advisory Group, aż 80% z ponad pięciu tysięcy przeanalizowanych CV zawierało przynajmniej jedną rozbieżność. Dane te korespondują z raportem pod nazwą "Kłamstwa w CV na polskim rynku pracy", opracowanym przez IBBC Group i Background Screening Service, zgodnie z którym aż 81% organizacji padło ofiarą oszustwa w CV lub złapało sprawcę takiego oszustwa na gorącym uczynku.

Komórki, do których składane są aplikacje zawierające kłamstwa, to najczęściej: działy sprzedaży (60,3%), działy administracyjne (29,7%), działy produkcji (31,4%) oraz działy finansowe (18,2%). Co symptomatyczne, te same komórki nieodmiennie wymieniane są w każdym niemal badaniu dotyczącym występowania poważnych nadużyć finansowych w organizacjach. I nie jest to przypadkowa korelacja.

Kłamstwa mogą pojawiać się w dokumentach aplikacyjnych składanych na praktycznie każde stanowisko – od pracownika fizycznego do prezesa zarządu. Jedni kandydaci tylko nieznacznie upiększają swoje kwalifikacje, by sprostać wyśrubowanym wymaganiom, inni fabrykują cały swój życiorys: **posiadane stopnie naukowe, historię zatrudnienia, posiadane certyfikaty i licencje, a nawet przebieg życia rodzinnego**. Jak wynika z przywołanego wcześniej raportu, kłamstwa dotyczą jednak najczęściej dodatkowych umiejętności – ten obszar wskazało aż 85,1% respondentów. Kolejne obszary to: **okres zatrudnienia w poprzednich firmach (58,7%), zakres wykonywanych tam obowiązków (53,7%), zajmowane wcześniej stanowisko (28,9%) oraz zdobyte wykształcenie (23,1%).**

Oszustom sprzyja postęp technologiczny – sfałszowanie dokumentu nie stanowi obecnie żadnego wyzwania, nie wiąże się także z koniecznością ponoszenia wysokich nakładów finansowych.

W większości przypadków wystarczy darmowy program graficzny oraz zwykła drukarka.

KONSEKWENCJE ZANIECHANIA

Pewne niedociągnięcia w składanych dokumentach to rzecz normalna, wszyscy zdążyli się już do nich przyzwyczaić i na nikim nie robią one chyba większego wrażenia. Czym innym jest jednak nieznaczne podkoloryzowanie swoich umiejętności, a czym innym sfałszowanie dyplomu czy zatajanie wyroku za udział w przestępstwie korupcyjnym. By zobrazować szkody, jakie mogą wynikać z braku weryfikacji informacji przedstawionych przez kandydata, wystarczy wyobrazić sobie zatrudnienie na stanowisku głównego księgowego osoby, która w poprzedniej pracy przez lata przywłaszczała sobie środki należące do pracodawcy.

Konsekwencje bywają zatem poważne: od nieprofesjonalnej realizacji zadań i zmniejszenia produktywności organizacji, poprzez frustrację i obniżone morale pracowników, po te najgroźniejsze: działanie na szkodę pracodawcy, kradzież danych, ustawianie przetargów, oszustwa, a także współpraca z konkurencją. Brak bowiem wymaganych kwalifikacji nie jest największym problemem. Jest nim nieuczciwość potencjalnego współpracownika. Jeśli osoba taka oszukała, aplikując o pracę, to skąd pewność, że nie oszuka raz jeszcze, kiedy już pracę tę zdobędzie?

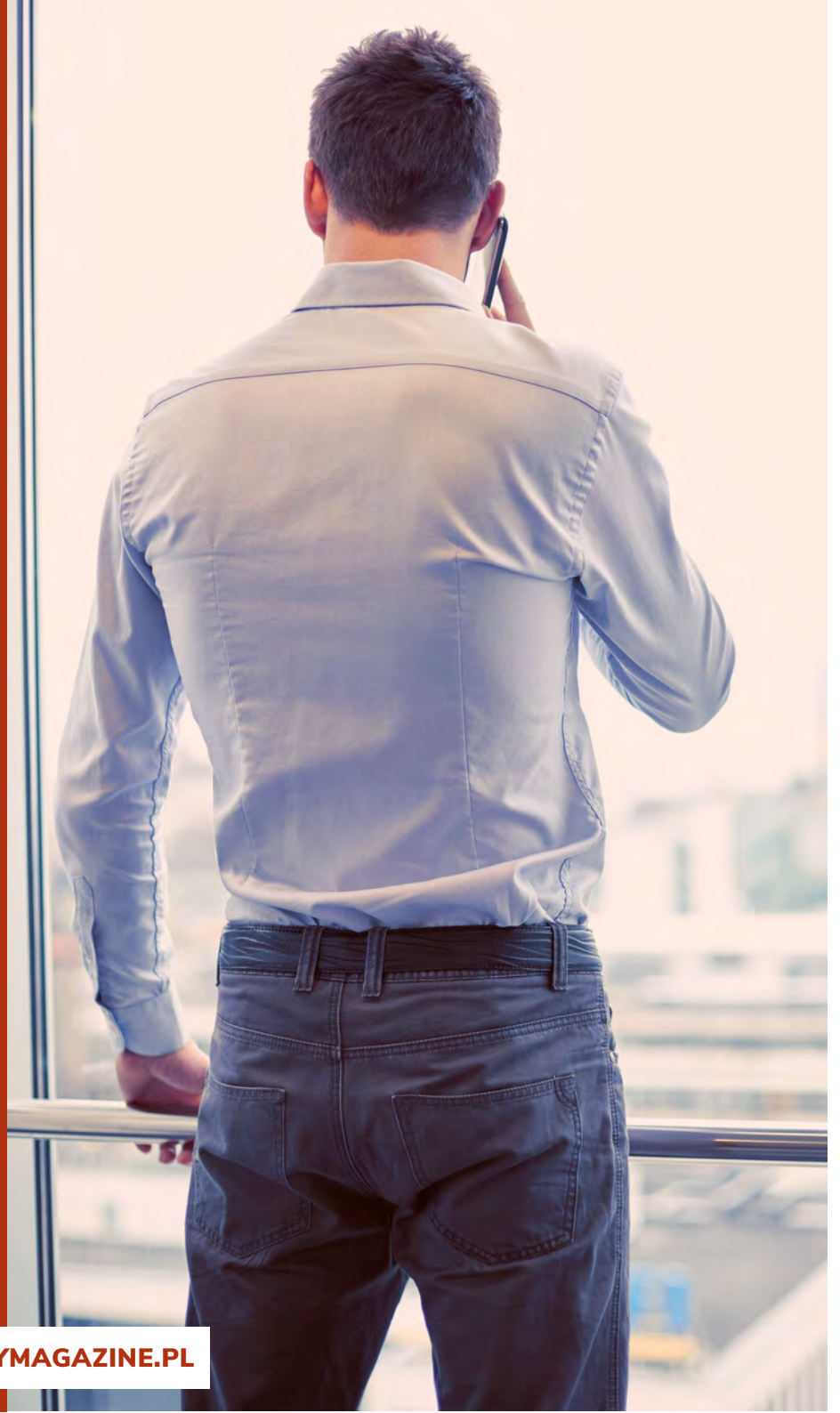
WERYFIKACJA

Jeśli więc uwzględnimy zagrożenia, jakie może nieść za sobą zatrudnienie nieuczciwej osoby, stwierdzimy, że weryfikacja przedstawionych wraz z CV dokumentów i informacji w nich wskazanych to nie kaprys, ale sposób na wyeliminowanie poważnego ryzyka.

Część kłamstw, zwłaszcza tych dotyczących konkretnych umiejętności, łatwo zweryfikować podczas rozmowy kwalifikacyjnej (na przykład poprzez proste testy umiejętności), w końcu temu właśnie służą rozmowy kwalifikacyjne. Problemy zaczynają się w przypadku deklaracji, których za pomocą testów sprawdzić nie sposób: **formalne wykształcenie kandydata, jego historia zawodowa, uczciwość czy przeszłość kryminalna.**

A te zagadnienia, zwłaszcza w przypadku stanowisk, które wymagają zaufania lub specjalistycznych umiejętności, często decydują o bezpieczeństwie organizacji.

Część informacji sprawdzić można na podstawie dokumentów wymaganych w procesie rekrutacji. Mimo - wydawałoby się - oczywistości takiego rozwiązania, niejednokrotnie już na tym etapie we-



ryfikacji okazuje się, że informacje w CV nie wytrzymują próby. Warto więc poprosić o przedstawienie stosownej dokumentacji i poświęcić jej chwilę.

Przebieg zatrudnienia zweryfikować można przez kontakt z poprzednim pracodawcą, należy jednak pamiętać, że nie zawsze jest to wiarygodne i obiektywne źródło. Pracodawca może mieć bowiem uraz do pracownika, który zrezygnował z pracy, a powodem takiej rezygnacji może być na przykład niewłaściwe środowisko pracy lub inne powody leżące po stronie pracodawcy. Należy mieć to na uwadze. Kontaktując się z byłym pracodawcą, warto korzystać z danych teleadresowych umieszczonych na oficjalnej stronie internetowej, nie tych podanych przez kandydata – te bowiem mogą kierować do osoby pozostającej w nim z zmowie.

Przebieg kariery zawodowej zbadać można również na popularnych zawodowych serwisach społecznościowych. Profil kandydata, wykształcenie, okresy zatrudnienia, uzyskane certyfikaty, nawiązywane kontakty, aktywność, poruszane zagadnienia czy sposób prowadzenia dyskusji również pozwalają na weryfikację informacji wskazanych w dokumentach aplikacyjnych.

Obszernym źródłem wiedzy są ogólnodostępne rejestry publiczne. Informacje zawarte w Centralnej

Ewidencji i Informacji o Działalności Gospodarczej, Krajowym Rejestrze Sądowym, Krajowym Rejestrze Zadłużonych, rejestrach branżowych i komercyjnych wywiadowniach gospodarczych pozwolą ustalić między innymi, czy kandydat nie prowadzi konkurencyjnej działalności, nie jest powiązany kapitałowo lub osobowo z konkurencją czy też nie jest niewypłacalnym dłużnikiem w związku z prowadzoną wcześniej działalnością gospodarczą. Informacje zawarte w ogólnodostępnych rejestrach, zwłaszcza w przypadku rekrutacji na stanowiska wrażliwe, mogą uchronić organizacje przed podjęciem katastrofalnej w skutkach decyzji. Informację o niekaralności kandydat przedstawić musi sam, pracodawca nie ma bowiem wglądu do Krajowego Rejestru Karnego.

O CZYM NALEŻY PAMIĘTAĆ

Background screening to nieustanne lawirowanie pomiędzy uprawnieniami wynikającymi z zapisów art. 22-1 §5 Kodeksu Pracy, zgodnie z którym pracodawca ma prawo żądania

udokumentowania danych przedstawionych przez kandydata w formie oświadczenia, a zapisami rozporządzenia o ochronie danych osobowych (RODO), istotnie zawężającymi możliwość weryfikacji informacji obejmujących te dane.

Dlatego o planowanym background screeningu należy poinformować już w ogłoszeniu o pracę, zawiadomić kandydatów, że oferta zatrudnienia uzależniona jest od przeprowadzonej weryfikacji i uzyskać ich pisemną zgodę na procedury z nią związane.

Należy również pamiętać, by podczas analizowania danych nie wykraczać poza niezbędne informacje, by nie narazić się na kosztowne procesy i kary. Decyzje Urzędu Ochrony Danych Osobowych bywają bowiem niezwykle surowe.

Wartością dodaną umieszczenia informacji w ogłoszeniu o pracę o planowanej procedurze background screeningu jest to, że już sama ta informacja skutecznie zniechęca potencjalnych oszustów do złożenia dokumentów w odpowiedzi na to ogłoszenie.

IV KONFERENCJA

POLSKA IZBA PRODUCENTÓW URZĄDZEŃ I USŁUG NA RZECZ KOLEI

BEZPIECZEŃSTWO NA KOLEI

8-9 grudnia 2022 r.

Hotel NADMORSKI
Gdynia

PATRONAT
SECURITY MAGAZINE

IV KONFERENCJA
BEZPIECZEŃSTWO NA KOLEI
8-9 GRUDNIA

WŚRÓD GOŚCI MIĘDZY INNYMI:

- Państwowa Komisja Badania Wypadków Kolejowych – Tadeusz Ryś
- Akademia Marynarki Wojennej – dr hab. Grzegorz Krasnodębski prof. AMW
- Polskie Koleje Państwowe S.A. – Rafał Zgorzelski
- Instytut Kolejnictwa – Andrzej Massel
- PKP Informatyka Sp. z o.o. – Tadeusz Turzyński
- PKP S.A. – Centrum Bezpieczeństwa Dworców Kolejowych – Michał Zagalski
- NASK-PIB – CERT Polska – Krystian Szefler
- PKP Szybka Kolej Miejska w Trójmieście sp. z o.o. – Grzegorz Przysiężny – Komendant SOK
- Komenda Główna Straży Ochrony Kolei – Adam Morawski

Zapraszamy do udziału w IV Konferencji „BEZPIECZEŃSTWO NA KOLEI”, która odbędzie się w Gdyni 8-9 grudnia 2022 roku w Hotelu Nadmorskim. Zachęcamy do uczestnictwa w konferencji w formie słuchacza, prezentacji multimedialnej promującej rozwiązanie oraz uczestnictwa w wystawie rozwiązań i usług.

Panele, debaty i prezentacje z udziałem polskich i zagranicznych gości będą skupiały się na tematyce cyberobrony w aspekcie wojskowym i cywilnym, prywatności danych, roli dyplomacji w branży cyberbezpieczeństwa, sztucznej inteligencji czy suwerenności w kontekście gospodarki cyfrowej.

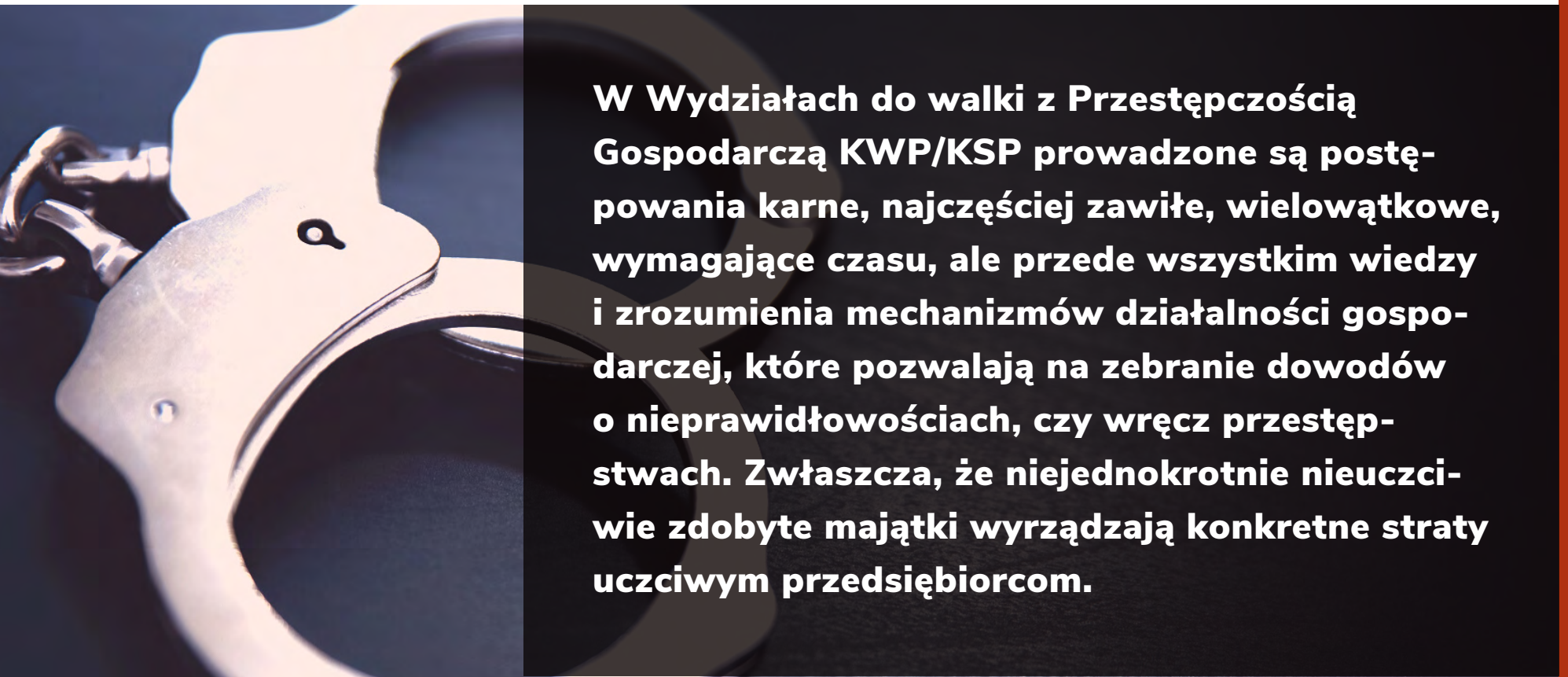
Zakres tematyczny konferencji:

- Prawo – procedury, przepisy, instrukcje, certyfikacja i akredytacja
- Zarządzanie bezpieczeństwem – SMS, oraz ryzykiem
- Bezpieczeństwo ruchu pociągów (ERTMS, przejazdy, urządzenia srk, automatyka, systemy wspomagające, łączność)
- Mobilny i stacjonarny monitoring wizyjny, drony, urządzenia dostępowe
- Bezpieczeństwo kolejowej infrastruktury energetycznej i transportowej
- Cyberbezpieczeństwo i ochrona danych (podatności, luki, środki naprawcze, monitoring procesów, nadzór)
- Inteligentne systemy informacji pasażerskiej
- Pojazdy szynowe – monitorowanie poziomów utrzymania, systemy bezpieczeństwa w taborze
- Współpraca służb (SOK, POLICJA, STRAŻ POŻARNA, Służby Ratownicze, Kolejowe Ratownictwo Techniczne)
- Infrastruktura dworcowa i przestrzeń publiczna – bezpieczny pasażer i pierwsza pomoc.

POBIERZ KARTĘ ZGŁOSZENIA

OSZUSTWA NA UCZCIWYCH PRZEDSIĘBIORCACH

insp. dr Mariusz Ciarka
Komenda Główna Policji



W Wydziałach do walki z Przestępczością Gospodarczą KWP/KSP prowadzone są postępowania karne, najczęściej zawiłe, wielowątkowe, wymagające czasu, ale przede wszystkim wiedzy i zrozumienia mechanizmów działalności gospodarczej, które pozwalają na zebranie dowodów o nieprawidłowościach, czy wręcz przestępstwach. Zwłaszcza, że niejednokrotnie nieuczciwie zdobyte majątki wyrządzają konkretne straty uczciwym przedsiębiorcom.

Podmioty, które padły ofiarą oszustwa, powinny jak najszybciej zgłosić takie zdarzenie na Policji albo w prokuraturze.

Można wysłać pocztą, mailem, faksem czy też przynieść osobiście do jednostki Policji napisane przez siebie zawiadomienie o przestępstwie.

TAK DZIAŁAJĄ OSZUŚCI

Przykładem takich postępowań, są dwa śledztwa nadzorowane przez prokuratorów z Prokuratury Okręgowej w Toruniu i Prokuratury Okręgowej w Bydgoszczy.

Choć są to różne postępowania, to sposób działania sprawców był bardzo podobny. Oszuści działali w branży spedycyjnej i transportowej. Na początku wyszukiwali osoby, które zgadzały się założyć na siebie firmę. Po znalezieniu tak zwanych słupów faktyczni sprawcy nie byli w żaden sposób powiązani z tymi firmami. Następnie na spółki te wynajmowali i urządzali pomieszczenia biurowe, zakładali strony internetowe, tworzyli logo firmy, a nawet zatrudniali pracowników.

Kolejnym krokiem było zdobycie pozytywnych opinii na temat założonych firm na portalach internetowych. Czynili to poprzez realizację usług, z których się faktycznie rozliczali. Niestety, do czasu. Po uzyskaniu odpowiedniej ilości pozytywnych opinii, zaczynali swoją faktyczną działalność. W ten sposób uwiarygodniona na rynku firma, z zamiarem, że tym razem nie wywiąże się z płatności, przyjmowała nowe zlecenia transportowe od zagranicznych kontrahentów, od których od razu otrzymywała zapłatę. Za wykonanie zlecenia polskim podwykonawcom już, niestety, nie płacono. Sprawcy wykorzystywali przyjęty zwyczajowo w tej branży, 60-dniowy lub dłuższy okres rozliczeniowy. W efekcie przez ten czas pokrzywdzeni nie byli świadomi, że padli ofiarą oszustwa. Dopiero po ponad dwóch miesiącach firmy orientowały się, że zostały oszukane.

SŁUPY I CZAS ŻNIW

Ten dwumiesięczny termin odroczonej płatności to był czas „żniw” dla obu zorganizowanych grup przestępczych. **W tym czasie sprawcy dokonywali transferów pieniędzy z kont firmy - słupa na inne konta bankowe,** skąd pieniądze były wypłacane za pomocą BLIK-a.

Następnie oszuści kończyli działalność, pozostawiając osobę, która użyczyła danych do założenia firmy z długami, a sami uaktywniali następną spółkę „słup”.

Ustaleni przez policjantów Wydziału dw. z Przestępczością Gospodarczą KWP w Bydgoszczy sprawcy to członkowie dwóch zorganizowanych grup przestępczych, którzy, mając na celu popełnianie przestępstw, doprowadzali w okresie od co najmniej 10 stycznia 2018 roku do 17 listopada 2021 roku do niekorzystnego rozporządzenia mieniem, poprzez celowe nieregulowanie należności.

Tym doprowadzili do strat nie mniejszych niż 4 miliony złotych na szkodę setek polskich firm. Funkcjonariusze docierają do kolejnych pokrzywdzonych, dlatego kwota ta cały czas rośnie.

W śledztwie nadzorowanym przez prokuratora Prokuratury Okręgowej w Toruniu sprawcy działali za pośrednictwem podmiotu z Grudziądza. Z kolei w śledztwie

nadzorowanym przez prokuratora Prokuratury Okręgowej w Bydgoszczy sprawcy działali za pośrednictwem, aż 26 podmiotów tak zwanych słupów z Bydgoszczy, Poznania, Katowic, Gdańska, a nawet Estonii i Słowacji.

ZATRZYMANIA, ZARZUTY

Od listopada 2021 roku do lipca 2022 roku policjanci Wydziału do Walki z Przestępczością Gospodarczą KWP w Bydgoszczy, przy wsparciu policjantów z miejscowych jednostek, zatrzymali łącznie 35 członków dwóch zorganizowanych grup przestępczych. Podczas czynności związanych z zatrzymaniami, przeszukaniami miejsc i doprowadzeniami zaangażowanych było każdorazowo od 60 do 100 policjantów.

Prokuratorzy wydali postanowienia o przedstawieniu zatrzymanym zarzutów dotyczących m.in. udziału z zorganizowanej grupie przestępczej dokonującej oszustw znacznej wartości. Wobec 5 podejrzanych Sąd Rejonowy w Bydgoszczy zdecydował o aresztowaniu. Wobec pozostałych zastosowano dozór policji, zakazy opuszczania kraju i poręczenia majątkowe od 10 tys. nawet do 100 tys. złotych.

Na uwagę zasługuje fakt, że policjanci i prokuratorzy ustalili nie tylko członków zorganizowanych grup przestępczych, ale i osoby, które kierowały tą działalnością. Za zarzucone podejrzanym przestępstwa grozi kara do 10 lat pozbawienia wolności.

W toku śledztwa sprawcom zabezpieczono mienie w postaci nieruchomości, luksusowych pojazdów oraz pieniędzy. Aktualnie analizowane są inne postępowania prowadzone przez jednostki na terenie całego kraju

pod kątem ewentualnego ich włączenia do opisanych spraw, biorąc pod uwagę odpowiedzialność karną, a także materialną oszustów.

W sprawach dotyczących przestępczości gospodarczej niezwykle ważne jest przejmowanie od sprawców nieruchomości, pieniędzy, samochodów czy innych luksusowych dóbr, w których posiadanie weszli w sposób nielegalny, czyniąc konkretne, wymierne szkody uczciwym przedsiębiorcom.

Opisane śledztwa trwają, a policjanci i prokuratorzy ciągle docierają do kolejnych pokrzywdzonych.

Jeśli zdecydowałeś się napisać zawiadomienie o przestępstwie samodzielnie, musisz pamiętać, że powinno ono spełniać wymogi pisma procesowego, wynikające z art. 119 k.p.k. To znaczy, że powinno zawierać w szczególności:

- oznaczenie organu, do którego jest skierowane (oznaczenie jednostki Policji lub prokuratury z adresem),
- dane personalne oraz adres wnoszącego pismo,
- opis sprawy, której dotyczy zawiadomienie (z uzasadnieniem),
- datę i podpis składającego zawiadomienie.

Zadbaj o potwierdzenie wysłania swojego zawiadomienia lub pokwitowanie, jeśli doręczyłeś je osobiście. Pokwitowanie z reguły będzie wiązało się z potwierdzeniem na kopii lub kserokopii Twojego zawiadomienia (z naniesioną datą i podpisem osoby przyjmującej).

W TWOJEJ FIRMIE
ZDARZYŁ SIĘ

WYCIEK DANYCH OSOBOWYCH?

MOŻEMY CI POMÓC

SPRAWDŹ JAK

Polityka® Bezpieczeństwa

SECURITYMAGAZINE.PL

BUDUJMY WSPÓLNIE LOKALNE BEZPIECZEŃSTWO. 23. KONFERENCJA BRANŻY OCHRONY

PATRONAT
SECURITY MAGAZINE

Fot. FLC Studio Dariusz Konsek

Podczas konferencji dyskutowano na ważkie tematy związane z branżą security, skupione wokół roli samorządu w zapewnieniu bezpieczeństwa lokalnego. Rozmawiano m.in. o technologiach dla miejskiego bezpieczeństwa, współpracy z mieszkańcami i partycypacji społecznej w tworzeniu bezpiecznych przestrzeni.

Fot. FLC Studio Dariusz Konsek (2)

MERYTORYCZNIE

- Mamy przekonanie, że lokalny poziom bezpieczeństwa – gmina, miasto, powiat i metropolie to kluczowe obszary aktywności administracji, przede wszystkim samorządowej oraz Policji, służb i straży podejmujących codzienny wysiłek zmierzający do ograniczania zagrożeń dla mieszkańców, zapobiegania kryzysom i właściwego reagowania w przypadku identyfikacji niebezpieczeństw - zapowiadała wydarzenie Polska Izba Ochrony.

Konferencje oficjalnie otworzyli: Jacek Jaśkowiak, Prezydent Miasta Poznania oraz Generał broni oraz Dowódca Wojsk Lądowych RP w latach 2006-2009, Waldemar Skrzypczak.

Wydarzenie zgromadziło wybitnych znawców tematyki bezpieczeństwa, zarówno praktyków jak i teoretyków. Obfitowało nie tylko w wiele merytorycznych prezentacji, ale i wartościowe debaty. Jednym z istotnych paneli dyskusyjnych była rozmowa ekspertów na temat współpracy prywatnego sektora ochrony z samorządami lokalnymi.

Fot. FLC Studio Dariusz Konsek (4)

Uczestniczyli w nim m.in.:

- **ppłk rez. dr inż. Tomasz Białek** - były oficer wojskowych jednostek specjalnych, Biura Ochrony Rządu i Centralnego Biura Antykorupcyjnego.
- **dr Natalia Moch** - Zastępca dyrektora ds. naukowych, Instytutu Bezpieczeństwa i Obronności Wojskowej Akademii Technicznej,
- **Sylwester Szczepaniak** - Koordynator ds. społeczeństwa informacyjnego i smart city w Biurze Unii Metropolii Polskich,
- **Artur Hołubiczko** - Prefekt Krajowej Rady Komendantów Straży Miejskich i Gminnych Rzeczypospolitej Polskiej
- **Prof. dr hab. Waldemar Zubrzycki** - Wyższa Szkoła Policji w Szczytnie.

Było to doskonałe wprowadzenie do serii merytorycznych wykładów, podczas których praktycy dziedziny bezpieczeństwa przybliżyli uczestnikom konferencji najnowsze rozwiązania technologiczne, które są użyteczne dla miejskiego bezpieczeństwa. Co istotne, konferencja łączyła w sobie wymiar praktyczny z wymiarem naukowym. Pozwoliło to na wymianę doświadczeń biznesu i aktywną rozmowę ze środowiskiem samorządów lokalnych, wymianę doświadczeń i spostrzeżeń.

Zaprezentowano na niej w sposób bardzo szeroki aktualne trendy i kierunki rozwoju branży security w Polsce i na świecie.

Fot. FLC Studio Dariusz Konsek (3)

Fot. FLC Studio Dariusz Konsek (4)

Fot. FLC Studio Dariusz Konsek (2)

Organizatorem wydarze nia była Polska Izba Ochrony Osób i Mienia (PIO). To jedna z wiodących organizacji przedsiębiorców zrzeszająca około 180 firm działających w branży bezpieczeństwa.

Partnerami Honorowymi oraz Merytorycznymi wydarzenia byli:

- Unia Metropolii Polskich im. Pawła Adamowicza,
- Związek Województw Rzeczypospolitej Polskiej,
- Local Trends,
- Securex,
- Stowarzyszenie Polskich Specjalistów Bombowych,
- Safety Project Jarosław Stelmach,
- RBS Rafał Batkowski Strategie.

POST MORTEM, CZYLI CO PO CYBERKRYZYSIE?

Beata Łaszyn
Alert Media Communications

Statystyki nieubłaganie wskazują olbrzymią liczbę cyberataków. Coraz więcej organizacji płaci okupy i coraz częściej tlą się lub wręcz szaleją kryzysy wynikające z ataków i niewłaściwych zabezpieczeń danych lub systemów IT. Potrzeba dobrej współpracy IT i PR-u w tym zakresie jest krytyczna, co jest widoczne podczas kryzysu. A już Winston Churchill mawiał: „Nie pozwól, aby dobry kryzys się zmarnował”.

Dziś już głośno mówi się o potrzebie bliskiej współpracy Bezpieczników (speców od cyberbezpieczeństwa) i PR-owców (speców od gry „w komunikację"). W uproszczeniu: jedni bez drugich nie będą mogli skutecznie wdrożyć zabezpieczeń w firmie bez dokładnego wyjaśnienia tego procesu, a drudzy nie będą potrafili skutecznie i sensownie komunikować.

Tak czy inaczej, spowoduje to, że organizacja znajdzie się (tak – nie może, ale na pewno) w olbrzymich tarapatach, że o pełnokrwistym kryzysie nie wspomnę. Bez tego porozumienia i współpracy dziś już chyba niemożliwe jest dobre zarządzanie – choćby dlatego, że kwestie bezpieczeństwa danych i systemów IT są obecnie jednymi z ważniejszych w biznesie i to dla wielu stron: od kontrahentów, przez klientów, na pracownikach kończąc.

Szczególnie teraz – kiedy wojna w Ukrainie pokazała, jak dużo mogą zdziałać hakerzy, a od czasu pandemii następuje lawinowy wzrost cyberprzestępczości. Polska jest przy tym szóstym najchętniej atakowanym krajem w Europie.

Kluczowymi elementami w obszarze komunikacji kryzysowej jest przygotowanie do sytuacji kryzysowych, działania stricte kryzysowe (te w oku cyklonu) oraz działania po kryzysie – bardzo często niewystarczająco realizowane, niedoceniane i ignorowane. Brak racjonalnych działań po kryzysie powoduje utratę cennych dla organizacji informacji i doświadczeń, co często oznacza, że pot i krew z placu boju idą w... piach, nie w żyzną glebę. A szkoda. Bo ciężar doświadczeń

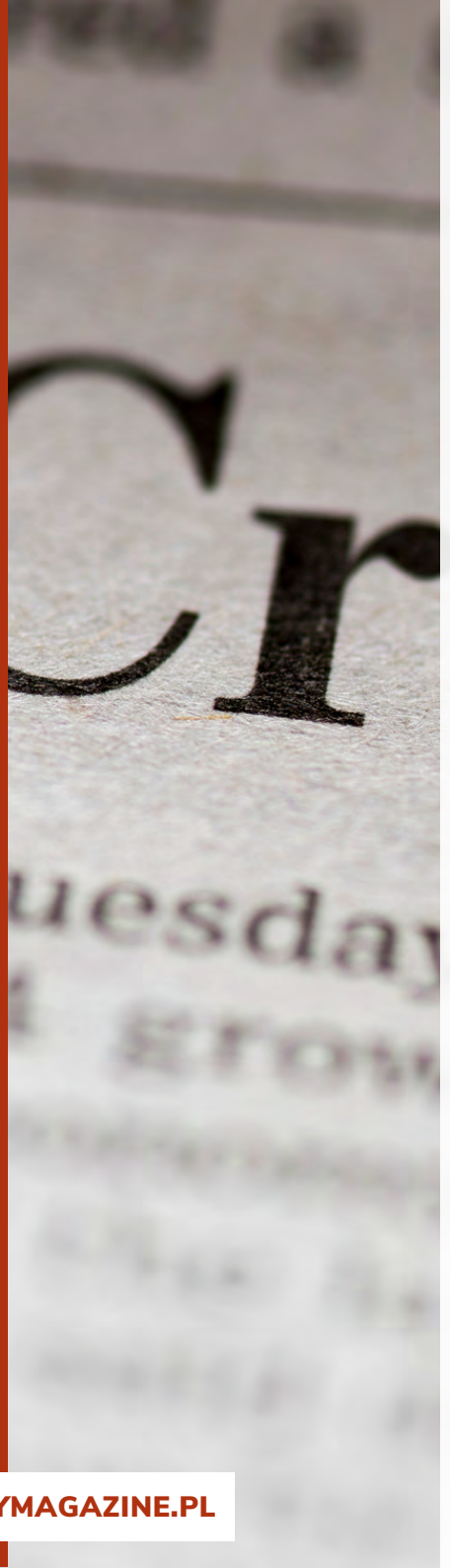
zasadniczo marnuje się i z powiedzenia „co nas nie dobije, to nas wzmocni" zostaje tylko kilka nic nieznaczących liter.

W Polsce, podobnie jak na całym świecie, lawinowo rośnie liczba cyberprzestępstw. Coraz częściej słyszymy o kolejnych atakach, okupach, przerażających statystykach. **Warto zatem przyjrzeć się działaniom POST MORTEM.** Dlaczego? Bo coraz więcej firm i organizacji jest lub zaraz będzie w tej sytuacji, a zdecydowanie mniej mówi się (i, niestety, robi) o działaniach pokryzysowych, o tym, co można i warto zrobić, jak już kurz bitewny opadnie, a straty zostaną policzone. A jest to cenna wiedza i doświadczenie, z których wiele można wyciągnąć. By jaśniej przedstawić i pokazać obie, tj. techniczną i komunikacyjną stronę medalu, pozwolę sobie obrazować tekst eksperckimi wypowiedziami z moich rozważań prowadzonych z Chief Security Officer (CSO) Błażejem Szymczakiem, przy okazji rozmów o koniecznej współpracy obu obszarów.

POST MORTEM – ALE O CO CHODZI?

Sformułowanie Post mortem pięknie określa i jednocześnie definiuje obszar działania oraz trudności.

Oddając głos Błażejowi Szymczakowi, to „działania po kryzysie. To nie tylko określenie, co zawiodło. Ważne jest ustalenie przebiegu kryzysu, reakcji właściwych i tych złych. Określenie słabych ogniw. Oraz, co krytyczne, wprowadzenie mechanizmów zmieniających słabe punkty. Nie można zostawić kryzysu bez działań naprawczych." Co ciekawe, ca-



ły cytat dotyczy zarówno obszaru technicznego bezpieczeństwa, jak i komunikacji! Wszystkie wymienione elementy stanowią część audytu pokryzysowego w warstwie komunikacyjnej. Kryzysy wizerunkowe, często towarzyszące problemom wewnętrznym i incydentom, które niekontrolowanie rozlewają się w przestrzeni publicznej,

ZAWSZE są spowodowane licznymi patologiami w komunikacji – zarówno zewnętrznej, jak i wewnętrznej – które nierzadko mogą zagrozić funkcjonowaniu firmy.

ZAWSZE JEST DWÓCH WINNYCH. CO NAJMNIEJ

Błażej Szymczak podsumował: „*W każdym, dosłownie w każdym incydencie zawodzą: komunikacja oraz monitoring. I każdy można tak podsumować, ale Post mortemy to wierzchołek góry lodowej, ponieważ zwykle dotyczą incydentów krytycznych. Natomiast całą resztę już należy postrzegać jako problem management - spojrzenie na incydenty niższego rzędu z lotu ptaka, znalezienie wspólnych mianowników i przyczyn, żeby to zrobić trzeba mieć spójną klasyfikację incydentów oraz ich odpowiednie oznaczanie, którego obszaru dotyczyły. Finalnie sprowadza się to do ustalenia, DLACZEGO tak się stało i jak możemy temu zapobiec w przyszłości. Chodzi o holistyczne spojrzenie na cała organizację, nie tylko wąski wycinek głównej akcji. Mechanizmy naprawcze również należy analizować i wdrożyć w holistycznym ujęciu.*” Jak poprzednio, to niemal lustrzane odbicie obszaru komunikacji. Dokładnie to samo można przeczytać w kontekście kryzysu wizerunkowego.

Dwa wyżej przytoczone cytaty, idealnie pasujące zarówno do przestrzeni cyberbezpieczeństwa, jak i komunikacji w organizacji, skłaniają do refleksji. Skoro cyberataki tak często zagrażają firmom i coraz częściej wiążą się z zagrażający kryzysami wizerunkowymi, to warto połączyć te dwa obszary i potraktować je podobnie. Choćby po to, żeby w przyszłości łatwiej było podnieść się po kryzysie i wyciągnąć więcej wniosków. Również po to, by doświadczania kryzysu przyczyniły się do minimalizacji błędów w przyszłości. A, jak mawiamy, kryzys to festiwal błędów.

DISASTER RECOVERY PLAN – WZÓR DO NAŚLADOWANIA

Standardy cyberbezpieczeństwa (choćby określone przez NIST, amerykańską agencją federalną wyznaczającej normy) zakładają, że jednym z elementów zapewnienia ciągłości działania jest Disaster Recovery Plan (dalej: DRP), a więc ustrukturyzowane podejście, które umożliwia organizacjom sprawne wznowienie pracy po incydencie IT.

Każda organizacja, oczywiście, musi dopasować działania i procedury do swoich warunków, jednak w pewnym uproszczeniu można określić parę obszarów wymagających uwzględnienia: od wskazania zespołu pracowników odpowiedzialnych za DRP, przez identyfikację krytycznych zasobów biznesowych, ocenę ryzyka i przygotowanie procedur, stworzenie kopii zapasowych krytycznych danych, po monitorowanie.

Pewnym benchmarkiem przyjętym na potrzeby mojego planu jest katalog zaproponowany przez Stefana Kaczmarka:

- zespół ds. odtwarzania awaryjnego,
- ocena ryzyka,
- spis wykorzystywanych urządzeń i programów: narzędzia zewnętrznych dostawców, sprzęt fizyczny, zasoby wirtualne, kluczowe dokumenty cyfrowe, elementy aplikacji czy bazy danych ze wskazaniem ich lokalizacji,
- identyfikacja krytycznych zasobów biznesowych,
- ustalenie celów planu odtwarzania po awarii,
- kopie zapasowe,
- testowanie i optymalizacja.

CRISIS RECOVERY PLAN

Odnosząc się do standardu DRP, można stworzyć analogiczną procedurę – Crisis Recovery Plan, która pomoże przeprowadzić bliźniacze działania w komunikacji (co również jest obszarem zalecanym do uwzględnienia przez NIST). Ułatwi ona synergię działania IT i PR w procesie Post mortem. Z tego powodu warto, by takie działania przebiegały w pewnej harmonii. Doświadczenia w komunikacji kryzysowej, obserwacje przebiegu wydarzeń oraz audyty pokryzysowe pozwoliły mi stworzyć schemat, który warto rozważyć w tego typu incydentach i kryzysach.

Działania prowadzone jednocześnie – synchronicznie – ułatwią całościowe wyciągnięcie wniosków, poprawienie procedur i unikanie błędów. Poniżej w ta-beli proponowany przeze mnie schemat Crisis Recovery Plan z odniesieniem do DRP.

POST MORTEM, czyli co po cyberkryzysie?

DISASTER RECOVERY PLAN (DRP)	CRISIS RECOVERY PLAN
Zespół ds. odtwarzania awaryjnego	1. Sztab pokryzysowy – wskazanie grupy ludzi odpowiedzialnej za stworzenie planu i systematyczne wdrażanie go. Sztab powinien działać niedługo po rozpoczęciu kryzysu, tak by miał wiedzę o działaniach, wydarzeniach i błędach. Ponieważ niektóre krytyczne błędy mogą leżeć po stronie zarządzających kryzysem, w zespole muszą być osoby mające odpowiednią pozycję do takiego feedbacku.
Ocena ryzyka	2. Analiza sekwencji zdarzeń – analiza przebiegu kryzysu, ocena środowiska wewnętrznego i zewnętrznego, szczególnie z uwzględnieniem możliwych przyszłych sekwencji zdarzeń i ewentualności powtórzenia sytuacji oraz błędów. W uproszczeniu – co się wydarzyło, co poszło nie tak – a co sprawdziło się, z analizą scenariusza oraz kluczowych momentów kryzysu.
Spis wykorzystywanych urządzeń i programów	3. Inwentaryzacja kanałów i źródeł komunikacji uczestniczących w kryzysie, szczególnie identyfikacja słabych ogniw (wraz z analizą ich negatywnego wpływu na sekwencje wydarzeń).
Identyfikacja krytycznych zasobów biznesowych	4. Identyfikacja zasobów – identyfikacja i analiza istniejących możliwości i zasobów zarówno po stronie adwersarzy, jak i sojuszników (również potencjalnych, np. niewykorzystanych w analizowanym przypadku).
Ustalenie celów planu odtwarzania po awarii	5. Ustalenie celów komunikacji oraz plan działań – określenie celów komunikacyjnych do osiągnięcia – konieczne, by wiedzieć, w jakim kierunku zmierzają działania.
Kopie zapasowe	6. Plan B – warto przygotować plan minimum, gdyby był wstrząs wtórny (często występujący w kryzysach mały nawrót negatywnych komentarzy, publikacji) lub dalsze problemy (nieprzewidziane dodatkowe komplikacje).
Testowanie i optymalizacja	7. Monitorowanie i ewaluacja – realizowane działania należy monitorować i w razie efektów oraz potrzeby zmieniać, dostosowywać do pojawiających się okoliczności i nowych elementów.

PRZED POST MORTEM – PRZEWROTNOŚĆ CZYNNOŚCI

Co wydaje się kluczowe, stworzenie ram Crisis Recovery Plan dobrze jest wykonać... przed kryzysem.

Dlaczego? Każdy, kto przeszedł kryzys (w zakresie bezpieczeństwa IT, jak i wizerunkowym) wie, że są to przejścia, o których najszybciej chcemy zapomnieć, zamknąć za sobą i zaliczyć do „przeszłości". Mniej lub bardziej poranieni chcemy iść dalej i nie grzebać w jeszcze gojących się ranach. Niestety, zdecydowanie warto to robić. Ustalenie działań RDC jest istotną częścią przygotowania bezpieczeństwa systemów – Bezpiecznicy mają to w dużej mierze uwzględnione i poukładane. Podobnie warto zrobić z Crisis Recovery Plan. Ustalić zasady, które w odpowiednim momencie zostaną rozpoczęte niemal automatycznie. Bez tego elementu ujęcia proceduralnego może się to nie udać.

Wiele moich doświadczeń wskazuje, że w sytuacjach, kiedy nie jest to zaplanowane, tylko niewielki odsetek organizacji decyduje się na takie działania. Powoduje to, że często powtarzają te same błędy, te same wadliwe reakcje, te same obszary tworzą te same problemy. Można oczywiście uderzać się co chwila w nadmiernie wystający róg stołu stojący w przejściu, tylko po co?

NIE TYLKO KOMPUTER MOŻE PAŚĆ OFIARĄ HAKERÓW

Redakcja
SECURITY MAGAZINE

W świadomości ukuło się, że tylko komputery są narażone na ataki cyberprzestępców – no i może jeszcze smartfony. To jednak nieprawda. Urządzeń, które mogą zostać zhakowane, jest znacznie więcej. Sprawdź, jaki sprzęt w Twojej firmie jest narażony na atak cyberprzestępców.

Nie tylko komputer może paść ofiarą hakerów

UWAŻAJ NA SWOJĄ DRUKARKĘ!

Biurokracja i administracja ciągle się w pełni nie scyfryzowały, a to oznacza jedno – tonę drukowanych papierów. W prawie każdej organizacji działa jakaś drukarka. Jednak czy wiesz, że jest ona prawdopodobnie narażona na atak hakerski? Jak podaje Zaufana Trzecia Strona, badacze z Uniwersytetu w Bochum udowodnili, że drukarki sieciowe mogą być podatne na ataki cyberprzestępców. Naukowcy przetestowali 20 różnych drukarek i okazało się, że praktycznie każda z nich miała przynajmniej jedną lukę, dzięki której możliwy był cyberatak. Niektóre miały ich nawet 12.

Jak wskazuje Zaufana Trzecia Strona, badacze przeprowadzili następujące ataki:

- DoS poprzez dwie linijki w PostScripcie powodujące wejście drukarki w niekończącą się pętlę;
- wymuszenie przejścia w tryb offline;
- fizyczne uszkodzenie poprzez zapisywanie długich nazw zmiennych do NVRAM. Ten ma ograniczoną żywotność liczoną w cyklach zapisu;
- podmianę polecenia wydruku strony na puste polecenie. Spowodowało to brak możliwości drukowania;
- zdalny reset do ustawień fabrycznych po SNMP;
- modyfikację czyichś zadań drukowania;
- zdalny odczyt danych z NVRAM;
- zdalny dostęp do systemu plików;
- przechwytywanie drukowanych dokumentów innych użytkowników;
- łamanie haseł PJL i PostScript.

Przetestowane urządzenia wypadły naprawdę kiepsko, jeśli chodzi o cyberbezpieczeństwo. Praktycznie na każdej drukarce możliwe było przeprowadzenie ataku nieskończonej pętli. Jedynie model HP LaserJet M2727nf się przed tym obronił. Drukarka po 10 minutach resetowała zadanie i była ponownie dostępna. Jednak w prawie każdym urządzeniu udało się uniemożliwić wydruki poprzez zmianę definicji drukowania strony. A co trzecią drukarkę można było przełączyć w tryb offline, a kilka modeli wręcz uszkodzić fizycznie przez 24-godzinną serię zapisów do NVRAM-u.

Rodzi się pytanie – dlaczego ktoś miałby zaatakować naszą drukarkę? To bardzo proste – te urządzenia podłączane są ciągle do internetu, a co więcej – do wielu komputerów czy smartfonów jednocześnie. Drukarki przetwarzają mnóstwo danych. Dzięki atakowi cyberprzestępca może wyciągnąć ważny dokument, uniemożliwić nam ich kopiowanie lub zmodyfikować zadanie i dorzucić własne treści do wydruku.

Wyobraź sobie sytuację, w której haker modyfikuje nr konta bankowego na fakturze. W ten prosty sposób Ty lub Twój klient możecie stracić mnóstwo pieniędzy. Możliwe nawet, że bezpowrotnie. Co więcej – niektóre drukarki mogą przechowywać więcej danych i informacji niż myślimy. Np. hasła do sieci WiFi, zabezpieczanych plików czy urządzeń, które sparowaliśmy. z drukarką.

Pozostaje pytanie, czy da się przed tym bronić. I cóż – owszem, da. Nie warto drukować wszystkiego przez WiFi czy NFC. Należy też rozejrzeć się za programami, które mogą dodatkowo zabezpieczać drukarki. Można też z urządzeniem sparować np. tylko jeden komputer, który nie pełni żadnej innej funkcji od drukowania – nawet łączenia się z internetem. No i, oczywiście – po prostu trzeba zachować zdrowy rozsądek.

KAMERY PRZEMYSŁOWE TEŻ MOGĄ PAŚĆ OFIARĄ HAKERÓW

O tym, że kamery można zhakować, niby wiemy, ale... ile firm czy prywatnych osób pozostawia standardowe hasła do kamer? Odpowiedź brzmi, dużo. Z kamerami jest o tyle problem, że nasze podejście do ich bezpie-

czeństwa jest mocno wybiórcze. Cała rzesza osób zakleja kamerki w laptopach, ale ile osób robi tak z przednimi aparatami w smartfonach? Ile osób odpina od komputera kamerki internetowe po skończonej wideokonferencji? Ile dba o bezpieczeństwo kamer przemysłowych w fabrykach czy domach?

W 2021 roku za oceanem wybuchła olbrzymia afera. Verkada, czyli startup dostarczający usługi kamer bezpieczeństwa dla wielu firm z Doliny Krzemowej, padł ofiarą ataku. Hakerzy uzyskali dostęp do 150 tys. kamer m.in. w fabrykach i magazynach Tesli, biurach Cloudflare, siłowniach Equinox, szpitalach, więzieniach, szkołach, posterunkach policji i w samej siedzibie Verkady. Oprócz dostępu do transmisji na żywo cyberprzestępcy uzyskali też dostęp do pełnego archiwum klientów startupu.

A to zaledwie jeden przykład. W zasadzie codziennie możemy przeczytać o zaatakowaniu jakichś kamer w firmach, publicznych placówkach czy domach prywatnych osób. A dzięki włamaniom cyberprzestępcy uzyskują dostęp nie tylko do transmisji na żywo. Mogą uprzykrzać nam życie na wiele sposobów. Wiele kamer przemysłowych ma wbudowane mikrofony i głośniki, dzięki czemu hakerzy mogą np. puszczać głośną muzykę albo inne dźwięki.

Tak działa np. patostreamer z Polski – Misterius. Osobnik ten od kilku lat uprzykrza życie ludziom na całym świecie. Misterius wchodzi na niezabezpieczone kamery CCTV i puszcza osobom

znajdującym się w domach, hotelach, firmach czy placówkach publicznych np. przemówienia Hitlera, dźwięki syreny alarmowej, odgłosy uprawianego seksu, wiertarki udarowej, pukania, awarii linii elektrycznej, dzwonienia telefonu, hymn ZSRR itd.

Patostreamer zgromadził prawie 25 tys. subskrybentów na You Tubie i działa w najlepsze.

A Ty i Twoja firma zdecydowanie nie chcecie dołączyć do grona osób, których kosztem bawi się on i jego widownia. A tym bardziej nie chcesz dołączyć do grona ofiar poważniejszych cyberprzestępców.

NAWET SAMOCHODY NIE SĄ BEZPIECZNE

W samochodach jest coraz więcej elektroniki. W zasadzie nowe auta to komputery na kółkach i tak jak ich stacjonarne odpowiedniki – mogą paść ofiarą cyberprzestępców. Zdolny haker może wyłączyć hamulce, silnik, systemy monitorowania ciśnienia w oponach, ogrzewanie lub klimatyzację. A nawet manipulować diagnostyką, odblokować lub zablokować drzwi, sterować wycieraczkami czy zmusić samochód do przyspieszenia.

Tak, to nie jest fikcja rodem z serii gier Watch Dogs. W 2022 roku 19-latek z Niemiec, David Colombo, włamał się do 25 samochodów Tesli. Dzięki uzyskaniu dostępu do systemów haker mógł odblokowywać drzwi, włączać radio, trąbić klaksonem, namierzyć lokalizację samochodu, a nawet uruchomić pojazd bez kluczyków. Na całe szczęście dla Tesli i właścicieli aut, Colombo jest ekspertem ds. cyberbezpieczeństwa, który chciał obnażyć słabe punkty elektrycznych samochodów. A zatem nikomu nie stała się krzywda. Jednak skoro on był w stanie to zrobić – to znaczy, że prawdziwy cyberprzestępca też byłby do tego zdolny.

A jak w ogóle możliwe było zhakowanie pojazdów? Colombo wskazał, że kwestia bezpieczeństwa dotyczyła sposobu, w jaki TeslaMate przechowywało informacje potrzebne do połączenia programu z samochodem. Co więcej – 19-latek znalazł błąd w oprogramowaniu producenta samochodu dla cyfrowego kluczyka samochodu. Co zresztą pozwoliło mu też pozyskać dane kontaktowe do właścicieli wspomnianych pojazdów.

Co możesz w takim razie zrobić, aby się chronić przed takimi atakami? Niestety, niewiele. Moc leży w producentach, którzy powinni dbać o cyberbezpieczeństwo swoich pojazdów.

Niemniej, możesz przynajmniej ograniczać systemy bezprzewodowe lub zdalne, które działają w Twoim samochodzie, nie używać przeglądarek dostępnych w systemach aut (bo te przeważnie są kiepsko zabezpieczone). I po prostu śledzić informacje dotyczące Twojego modelu pojazdu.

URZĄDZENIA IOT I IIOT SĄ BANALNE W ZHAKOWANIU

Internet rzeczy oraz przemysłowy internet rzeczy zmieniły pracę i codzienne życie wielu osób. Roboty sprzątające, smartlodówki i smartpralki, czujniki, lampy, termostaty, skanery, maszyny produkcyjne itd. itp. – wszystko to może zostać zhakowane. I jak wskazuje serwis Embedded Computing, większości urządzeń IoT brakuje jakichkolwiek zabezpieczeń. Przez to złamanie internetu rzeczy dla cyberprzestępców to bułka z masłem. Urządzenie IoT bez odpowiedniego zabezpieczenia może zostać zhakowane w ciągu kilku godzin, a bez minimalnej ochrony nawet w parę minut. Szacuje się, że w samym tylko 2021 roku ofiarom cyberprzestępców padło 1–1,5 mld urządzeń IoT.

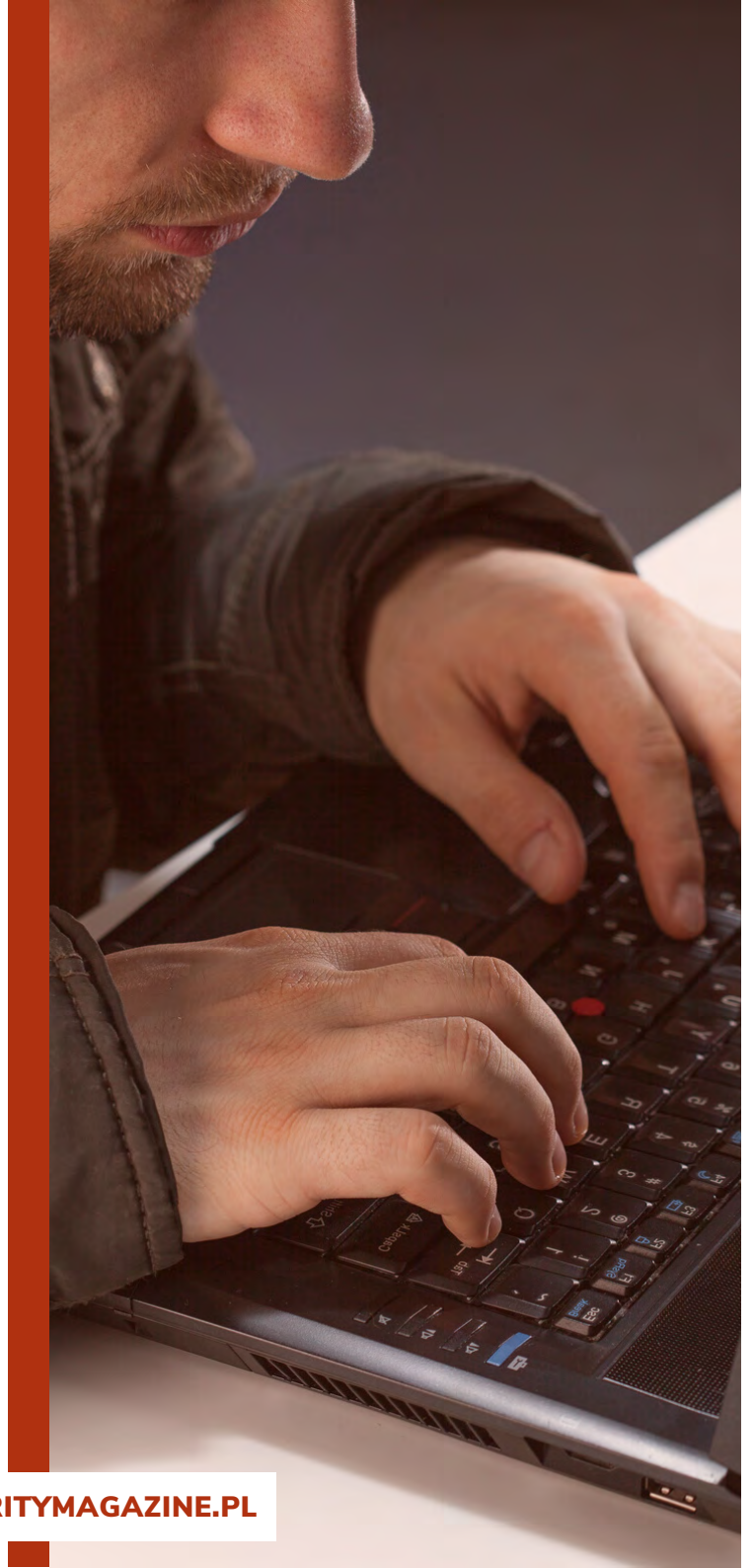
I co ciekawe, do prawie 900 mln tych ataków wykorzystywano metody phishingowe. Jeśli Twoja firma wykorzystuje internet rzeczy lub przemysłowy internet rzeczy, musisz mieć się na baczności.

Praktycznie wszystko, co jest podpięte do internetu, może paść ofiarą hakerów czy innych cyberprzestępców.

CYBERPRZESTĘPCY ATAKUJĄ RÓWNIEŻ DRONY

Bezzałogowe statki powietrzne też nierzadko są atakowane przez hakerów. Cyberprzestępcy zarówno kradną dane z dronów, np. zdjęcia czy filmy, a nawet same urządzenia. Porywanie tych małych statków powietrznych zdarza się naprawdę często. Niestety, producenci rzadko dbają o cyberbezpieczeństwo swoich produktów.

A wszyscy doskonale wiemy, że drony są coraz ważniejsze. Mają zastosowania bojowe, pomagają służbom znajdować ludzi w niebezpieczeństwie, służą do monitorowania okolicy, fotografują czy filmują ją, są wykorzystywane w celach marketingowych (np. w Szanghaju układają się w wielkie znaki QR na niebie), a w przyszłoś-



ci może zaczną w sposób powszechny dostarczać nam paczki.

Jak zatem hakerzy atakują drony? Np. podając im fałszywe dane GPS. Przez to dron zaczyna lecieć w zupełnie innym kierunku. Bezzałogowe statki powietrzne można zhakować nawet z odległości ponad 1,5 km. Wystarczy przechwycić sygnał drona, który często jest nieszyfrowany.

Samy Kamkar – ekspert ds. cyberbezpieczeństwa – zhakował drona, dzięki któremu mógł przechwycić też inne urządzenia tego typu. W konsekwencji utworzył prawdziwy „rój" dronów. I w zasadzie mógł z nimi zrobić, co chciał. Nie tylko je porwać, ale też np. rozbić o kogoś lub coś. Aby ustrzec się przed zhakowaniem drona, należy regularnie aktualizować jego oprogramowanie, używać mocnych haseł do aplikacji stacji bazowych i zabezpieczać urządzenia, za pomocą których sterujesz bezzałogowym statkiem.

Nie wymieniliśmy wszystkiego, co można by zhakować. W zasadzie urządzeń podatnych na ataki cyberprzestępców jest więcej. Ofiarami mogą padać też np. smart TV, automatyczne drzwi, asystenci głosowi, a nawet ekspresy do kaw.

Każde urządzenie podpięte do internetu, jest narażone na atak. A smutna prawda jest taka, że obecnie coraz więcej rzeczy korzysta z dostępu do sieci. Dlatego dbaj o cyberbezpieczeństwo swoje, swoich pracowników i firmy.

SECURITYMAGAZINE.PL

TAK RODZĄ SIĘ BIZNESY WSPIERAJĄCE... INNE BIZNESY. CARPATHIAN STARTUP FEST

PATRONAT
SECURITY MAGAZINE

Fot. CSF 2022

Druga edycja Carpathian Startup Fest 2022 wpisała się na listę najważniejszych imprez startupowych w Polsce. Do tegorocznej edycji zgłosiło się 226 projektów. 24 najlepsze pomysły biznesowe walczyły w finale o nagrody warte ponad 100 tys. zł, ale także o uwagę funduszy venture i potencjalnych inwestorów.

ŚWIAT STARTUPÓW W RZESZOWIE

Festiwal zorganizowany 13 i 14 października przez **Rzeszowską Agencję Rozwoju Regionalnego S.A. oraz Podkarpacki Park Naukowo-Technologiczny „Aeropolis”** przyciągnął uwagę młodych przedsiębiorców, biznesu, nauki, funduszy inwestycyjnych oraz firmy Kulczyk Investments SA, która jest twórcą mentoringowego InCredibles dla najbardziej innowacyjnych startupów.

Do Rzeszowa zjechały gwiazdy świata startupów: Stefan Batory, twórca aplikacji Booksy; Michał Sadowski, założyciel Brand24; Szymon Janiak, współtwórca Czysta3.vc – jednego z najbardziej aktywnych funduszy venture capital w Europie Środkowo-Wschodniej; Tomasz Karwatka, anioł biznesu, założyciel Catch the Tornado; Jarosław Sroka, członek zarządu Kulczyk Investments SA; Michał Kramarz, szef Google for Startups w Polsce oraz Katarzyna Cichopek, aktorka i prezenterka telewizyjna, założycielka marki „YA”.

NAGRODZENI

Rozdano nagrody w czterech kategoriach:

- **Najlepszy Startup** dla Visual Tech – Lab Sp. z o.o.;
- **Najlepszy Scaleup** i zwycięstwo firmy ParkCash Sp. z o.o.;

Patronat Security Magazine.
Carpathian Startup Fest

- **Najlepszy Pomysł na Biznes**, kat. Idea Challenge i zwycięski projekt MoVA;
- **Inteligentne Specjalizacje Województwa Podkarpackiego** dla Gridaly w obszarze „Informacja i telekomunikacja” oraz MoodMon w „Jakości Życia”.

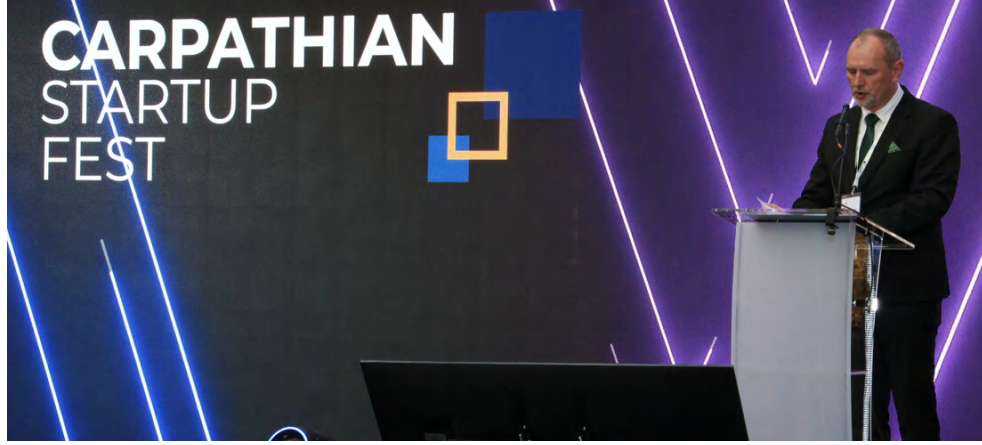
Po raz pierwszy w Rzeszowie wręczono nagrody dla Najlepszego Startupu z Ukrainy i otrzymał ją Vitaliy Rozman za aplikację Skibble oraz InCredibles Sebastiana Kulczyka, która trafiła do AstroTectonic Sp. z o.o.

NAJLEPSZE STARTUPY

Do tegorocznej edycji #CSF zgłosiło się 226 projektów. 24 najlepsze pomysły biznesowe walczyły w finale o nagrody warte ponad 100 tysięcy zł, ale też uwagę funduszy venture i potencjalnych inwestorów.

Najskuteczniejszy okazał się Visual Tech – Lab Sp. z o.o. założony przez Andrzeja Halarewicza i Marka Uziela. To oni wpadli na pomysł bezinwazyjnej oceny stanu gęstości kości pacjenta przed zabiegiem wszczepienia implantu. Drugie miejsce w kategorii Najlepszy Startup przypadło firmie AstroTectonic, która w 2020 powstała w PPN-T „Aeropolis” w Jasionce. Orteza na urazy przedramienia firmy Mediprintic sp. z o.o. zajęła trzecie miejsce w kategorii Najlepszy Startup.

AstroTectonic został też zakwalifikowany do prestiżowego pro-



Patronat Security Magazine.
Carpathian Startup Fest

Fot. CSF 2022

jektu InCredibles zainicjowanego w 2017 roku przez Sebastiana Kulczyka. To wszechstronny program akceleracyjno-mentoringowy wspierający młode polskie firmy z obszaru nowych technologii. Firma przez rok będzie za darmo korzystać ze wsparcia udzielanego przez polskich i zagranicznych mentorów – uznanych inwestorów, doradców i specjalistów z zakresu m.in. zarządzania, sprzedaży i marketingu, komunikacji, finansów oraz HR.

Projekt AstroTectonic ma na celu wykrywanie zagrożeń związanych z trzęsieniami ziemi i opracowanie optymalnego systemu powiadamiania dla ludności cywilnej oraz profesjonalistów, nawet kilka godzin przed wystąpieniem zagrożenia.

Jarosław Sroka, członek zarządu Kulczyk Investmens S.A., odpowiedzialny za InCredibles, nie kryje dumy z udziału w Carpathian Startup Fest 2022, tym bardziej, że tej współpracy towarzyszy pełne partnerstwo oraz założenie win win (wygrany-wygrany). - *Naszym wspólnym mianownikiem jest dobro polskiego ekosystemu startupowego* – mówił.

NAJLEPSZE SCALEUPY

W kategorii Najlepszy Scaleup - I miejsce zdobyła spółka ParkCash, która opracowała innowacyjną technologię zarządzania miejscami parkingowymi w biurowcach i obiektach handlowych.

Maas Loop z Rzeszowa, ubiegłoroczny zwycięzca Carpathian Startup Fest w kategorii Najlepszy Startup, w tym roku zajął II miejsce wśród najlepszych scaleupów. To nagroda za inteligentne kosze miejskie na szkło, plastik i aluminium. III nagroda trafiła do Battery Technic Sp. z o.o., która stworzyła domowy system zarządzania energią z magazynem energii.

Patronat Security Magazine.
Carpathian Startup Fest

GWIAZDY STARTUPOWEGO ŚWIATA

Carpathian Startup Fest 2022 na dwa dni ściągnął do Rzeszowa także gwiazdy startupowego świata. Obecny był Stefan Batory - twórca aplikacji Booksy dla klientów i przedsiębiorców, która jest na najlepszej drodze, by podbić światowe rynki i stać się równie rozpoznawalną i globalną marką jak Uber czy Booking. Co więcej, 44-letni Batory, który pochodzi z Kolbuszowej na Podkarpaciu, ma szansę zostać właścicielem polskiego jednorożca - startupu wycenianego na minimum miliard dolarów.

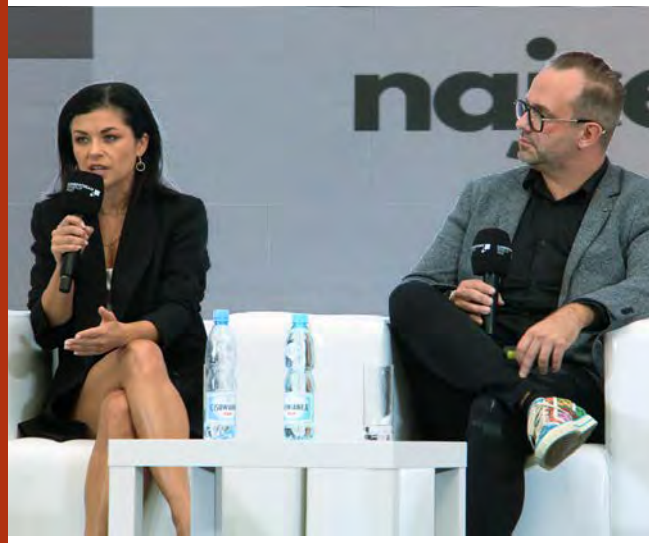
- Gdy 22 lata temu założyłem pierwszą firmę, przez 2 lata jadłem ziemniaki przez 6 dni w tygodniu, bo na nic innego nie było mnie stać – wspominał Batory: *- I gdybym wtedy wiedział, że tak będzie wyglądała moja droga do przedsiębiorczości, nigdy bym jej nie rozpoczął, ale nie wiedziałem. Dziś natomiast wiem, że było warto!*

- Obserwując InCredibles, wiem, że każdy nosi buławę Elona Muska w plecaku i namawiam przedsiębiorców do ciężkiej nauki. A idą trudne czasy dla przedsiębiorców. Wchodzimy w okres zawirowań i wyzwań gospodarczych związanych z recesją i inflacją. Kończą się pieniądze, inwestorzy mocno ograniczają swoje działania, cięcie kosztów i redukcja zatrudnienia mogą stać się koniecznością – wyliczał Jarosław Sroka.

INTELIGENTNE SPECJALIZACJE

Wręczono też nagrody w kategorii Inteligentne Specjalizacje Województwa Podkarpackiego. W obszarze „Informacja i tele-

Patronat Security Magazine.
Carpathian Startup Fest



komunikacja" wyróżniono platformę eventową Gridaly. W „Jakości Życia" MoodMon - aplikację do monitorowania osób z zaburzeniami afektywnymi. Po raz pierwszy w Rzeszowie podpisano Memorandum o współpracy pomiędzy West Ukrainian Business Club a RARR.

CYBERBEZPIECZEŃSTWO, IT I NOWE TECHNOLOGIE

Podczas prelekcji poruszone były również tematy związane z szeroko pojętym bezpieczeństwem, ale także z nowymi technologiami.

"Strategia cyberbezpieczeństwa. Rekomendacje w perspektywie XXI wieku" - podczas spotkania, które poprowadził dr Maciej Chrzanowski z Politechniki Rzeszowskiej rozmowa skierowana była wokół tego, na jakie zagrożenia w sieci mogą trafić nie tylko pracownicy firm czy administracji, ale też zwykły Kowalski, korzystający z internetu. Wątek omówili Michał Kibil - Senior Partner DGTL Kibil Piecuch i Wspólnicy S.K.A., Piotr Szymański - Naczelnik Centralnego Biura Zwalczania Cyberprzestępczości i Tadeusz Polak – CSO Ringer Axel Springer.

- Ważne byśmy wiedzieli, w jaki sposób możemy być atakowani, w jaki sposób możemy stać się ofiarami przestępstw, czy stalkingu internetowego, ale także w jaki sposób zabezpieczać się na poziomie prostej wiedzy użytkowania komputera i internetu. To jest podstawa edukacyjna i to, co mogą zrobić firmy, to wśród swoich pracowników dystrybuować materiały, uczyć, czym są kampanie phishingowe, a może przygotować materiały, które ci pracownicy będą mogli wziąć do domu i pokazać rodzinie, by szerzyć te informacje - podsumował spotkanie Maciej Chrzanowski.

Podczas prelekcji **"Telekomunikacja i informatyka. Obszar aktywności startupów"** gospodarz Krzysztof Szumilewicz ze Stowarzyszenia Informatyka Podkarpacka debatował z Wacławem Szarym, Członkiem Rady Nadzorczej Sagitum S.A., Markiem Pankiem, Wicepreze-

Patronat Security Magazine.
Carpathian Startup Fest

sem Zarządu Asseco Poland, Pawłem Jandą, Prezesem Zarządu Mobitouch i Tomaszem Jaworskim, Dyrektorem Transformacji Cyfrowej Sektora Publicznego Microsoft.

W czasie CSF poruszono również tematy związane z awarią terminala, czyli jak Operator Płatności może wpłynąć na Twój biznes. Tu uczestnicy wysłuchali prelekcji Adama Jastrowicza - Partnership Managera z Blue Media. O tym, jak usprawnić biznes czyli na temat współpracy z firmami w zakresie IT/HR mówiła Dominika Łuszczuk - Prezes Zarządu Vasco Sky sp. z o.o. A o tym, czym jest metaverse i jak na nim zarobić mówił Konrad Ziaja producent XR, założyciel i CEO CinematicVR. 11 lekcji z prowadzenia biznesu w Internecie zaprezentował Michał Sadowski - CEO & Head of Product Brand24 S.A. O technologii druku 3D, czyli geometrii bez granic opowiadał dr Piotr Wanicki – Co-Founder 3D House.

Carpathian Startup Fest to trzy różne sceny, a jedną z nich była **Deep Tech.** Przez dwa dni odbywały się prelekcje oraz warsztaty dla firm tworzących rozwiązania z dziedziny głębokich technologii. Firmy deep tech związane są z branżami AI i machine learning, syntezy mowy, zaawansowanej produkcji, robotyki, fotoniki, elektroniki, rozwiązań materiałowych, blockchain, biotechnologii i technologii kwantowych. To dla nich organizatorzy przygotowali debaty na temat danych (Paweł Lubiński – Data Scientist, Sagitum S.A), chmury obliczeniowej (Paweł Cisło – MLOps Engineer), rozwiązań mobilnych wspomaganych sztuczną inteligencją (Grzegorz Dworak – CTO projektu Mint Service Desk w firmie OPGK Software, robotyzacji i automatyzacji procesów (Paweł Lubiński – Data Scientist, Sagitum S.A). Warsztaty poprowadzili: Grzegorz Dworak – CTO projektu Mint Service Desk w firmie OPGK Software (“Rozwiązania mobilne z wykorzystaniem sztucznej inteligencji”), Gracjan Walczak – IT Project Manager CCC Group (“Zarządzanie projektem – frameworki i najlepsze praktyki”) czy Michał Blajer - Digital Robots sp. z o.o (“Robotyzacja & automatyzacja – zbuduj własnego bota”).

W tym roku organizatorzy CSF przygotowali także strefę Expo i Targi IT.

Patronat Security Magazine.
Carpathian Startup Fest

SECURITYMAGAZINE.PL

OCHRONA PRZED PODRÓBKAMI, BOTAMI I OPTY-MALIZACJA CYBERSEURITY

Redakcja
SECURITY MAGAZINE

Wiele startupów na rynku dostarcza rozwiązania, które pomagają chronić Ciebie i Twoją firmę. Mowa tutaj nie tylko o cyber-zagrożeniach, ale nawet ochronie przed podra-bianiem produktów. Na które startupy powinieneś zwrócić uwagę?

VERIORI – OCHRONA PRZED PODRÓBKAMI

Wywodzące się z Warszawy Verior S.A to startup, który dostarcza system potwierdzający autentyczność Twoich produktów. Działa on na podstawie kodów QR. Jednak po kolei – unikatowy identyfikator VAS umieszczany na każdym produkcie umożliwia śledzenie jego historii – od momentu powstania do zakupu przez klienta.

To ważne o tyle, że straty w samym tylko sektorze kosmetyków i higieny osobistej w 2019 roku wzrosły o 10,8 mld zł z powodu podróbek. A w 2020 roku łączną wartość rynku fałszywek w UE oszacowano na 121 mld euro.

Kody QR skanuje się za pomocą specjalnego czytnika lub aplikacji w smartfonie. Dzięki temu w łatwy sposób można potwierdzić autentyczność danego produktu.

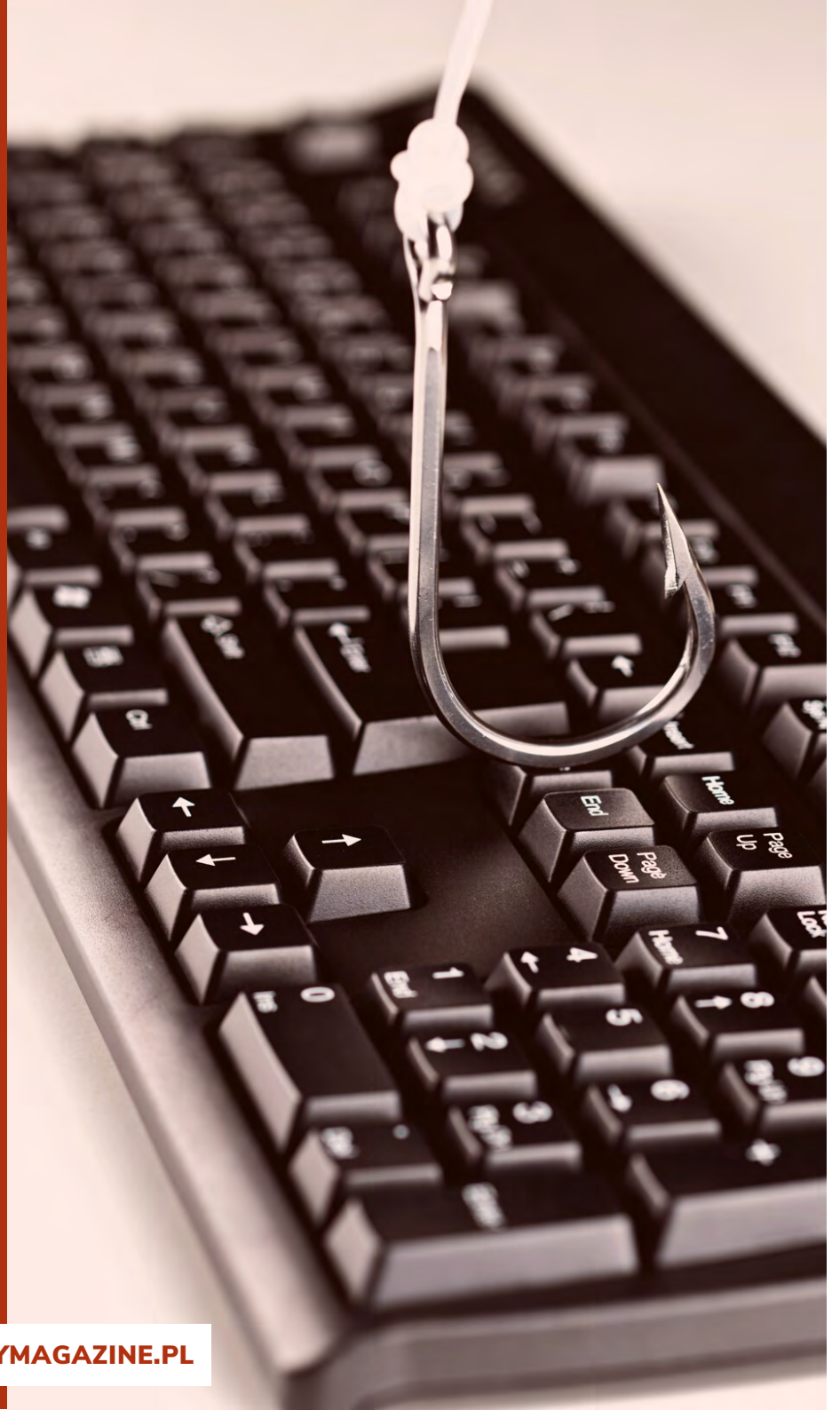
Zwyczajnie chroni Cię to przed powstawaniem i dystrybucją podróbek. Dzięki temu dbasz też o wizerunek uczciwego i rozsądnego producenta. Takiego, który potrafi ochronić siebie i swojego klienta. To jednak nie koniec. Identyifkator VAS pozwala także na zapisanie informacji, które mogą być przydatne do działań marketingowych. Skanowanie kodu QR ma też ułatwiać kontakt z obsługą klienta i upraszczać proces składania reklamacji czy wsparcia posprzedażowego. Identyfikatory umożliwiają również analizę danych, np. preferencji klientów, a nawet lokalizację i kontrolę łańcuchów dostaw.

Startup oferuje swoje rozwiązania zwłaszcza sektorowi FMCG, branży rolniczej, przemysłowi farmaceutycznemu czy producentom sprzętu medycznego. Niemniej, jak zapewnia Veriori – identyfikatory można dopasować praktycznie do dowolnej dziedziny.

W spółkę zainwestował m.in. fundusz Netrix Ventures. A sam startup współpracuje już, na przykład z IBM, Microsoftem, Zebra itd.

CYBER QUANT OCHRONI CIĘ PRZED PHISHINGIEM

Phishing to ciągle jedna z najpopularniejszych metod stosowanych przez cyberprzestępców. Cyber Quant wychodzi naprzeciw tym zagrożeniom. Warszawski startup tworzy platformę SEPP (Social Engineering Protection Platform), która ma na celu polepszanie kompetencji pracowników i przeciwdziałanie cyberprzestępstwom.



Jak wskazuje raport MIT w ciągu następnych 10 lat cyberatak i wycieki danych, będą jednym z największych zagrożeń na świecie. W zasadzie – już są niezwykle poważnym. Wszyscy słyszeliśmy historie o zatrzymanych liniach produkcyjnych czy sieciach energetycznych z powodu cyberprzestępstw. A aż 91% cyberataków zaczyna się właśnie od phishingu.

Startup pozwala na tworzenie symulacji cyberataków na poszczególne elementy, osoby w firmie. Po każdym takim kontrolowanym ataku, wdrażany jest moduł szkoleniowy i udostępniane podsumowanie.

Cyber Quant specjalizuje się też w OSINT, czyli tzw. białym wywiadzie. Jest to metoda pozwalająca na pozyskiwanie informacji o spółce czy osobie na podstawie jawnych źródeł. Startup dzięki temu wskazuje, które obszary powinieneś chronić w szczególności i gdzie znajdują się Twoje słabe punkty.

GREY WIZARD – ZABEZPIECZ SIĘ PRZED ZŁYMI BOTAMI I DDOSAMI

Ataki DDoS i złe boty to równie często wykorzystywane metody przez cyberprzestępców, co wspomniany wcześniej phishing. W ekosystemie startupowym jednak nie brakuje rozwiązań, które pozwalają

się chronić przed takimi zagrożeniami. Jedną ze spółek oferującą ochronę przed atakami DDoS i złymi botami jest Grey Wizard. To wywodzący się z Poznania startup, założony przez weteranów, którzy brali udział w rozwoju takich platform, jak Allegro czy OLX.

Grey Wizard oferuje całodobową ochronę działającą na zasadzie tzw. reverse proxy. Jest to serwer stojący pomiędzy użytkownikiem a infrastrukturą webową klienta. W końcu strony internetowe są dziś wyjątkowo narażone na cyberataki, a stanowią ważną część każdego biznesu. Rozwiązanie Grey Wizard blokuje złe boty, a przepuszcza tylko te dobre, np. od Google'a. Ponadto platforma chroni przed atakami DDoS i zapewnia bezpieczeństwo stron, aplikacji czy API.

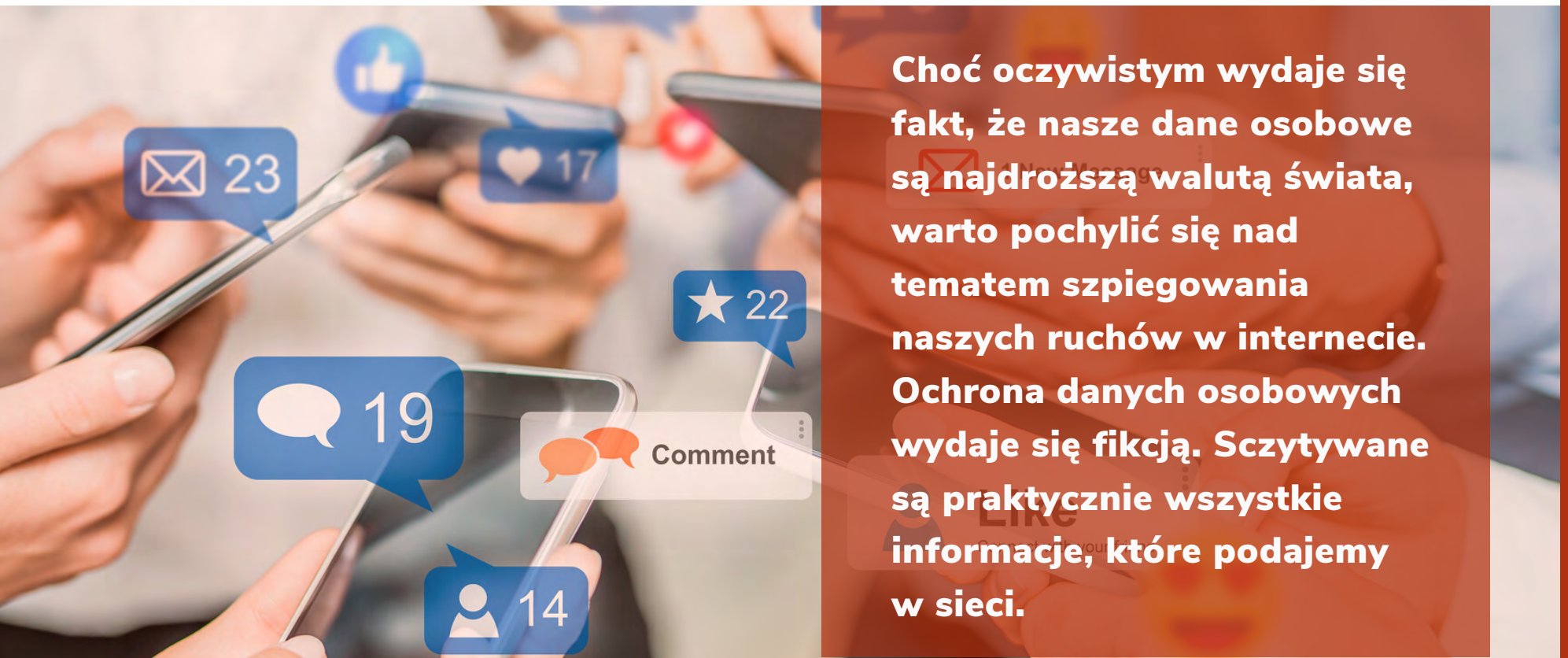
Startup chwali się tym, że na podłączenie i konfigurację ich narzędzia potrzeba zaledwie 5 minut. Ponadto Grey Wizard zapewnia szybki support i nie wymaga specjalnego sprzętu, oprogramowania czy ekspertów do obsługi platformy. Tarcza Grey Wizard przekierowuje ruch HTTP/HTTPS przez warstwę filtrującą, co w praktyce uniemożliwia ataki DDoS każdego rodzaju. Rozwiązanie oparte jest o uczenie maszynowe i sztuczną inteligencję, która stale się uczy.

Co więcej – startup oferuje monitoring w czasie rzeczywistym, który pozwala na podgląd parametrów sieci, użytkowników czy incydentów. Wszystko to w formie map i wykresów.
Z usług Grey Wizard korzysta już między inymi Wykop.pl, Smyk, Kinguin czy sklep jubilerski Savicki.

Startupów, które mogą zapewnić bezpieczeństwo Twojej firmie, jest znacznie więcej. To tylko kilka przykładów. Pamiętaj, aby dbać o dobro swojej spółki, jak i Twoje własne oraz pracowników.

CZY SOCIAL MEDIA NAS SZPIEGUJĄ?

Anna Petynia-Kawa
Agencja Kreatywna AjPi Media



Choć oczywistym wydaje się fakt, że nasze dane osobowe są najdroższą walutą świata, warto pochylić się nad tematem szpiegowania naszych ruchów w internecie. Ochrona danych osobowych wydaje się fikcją. Sczytywane są praktycznie wszystkie informacje, które podajemy w sieci.

JAKIE DANE OSOBISTE UDOSTĘPNIAMY SOCIAL MEDIOM?

Na początku, choć na chwilę wrócę myślami do pandemii i pierwszych teorii spiskowych związanych z mikroczipami. Kiedy ktoś mówi, że nie chce być śledzony, zawsze żartobliwie odpowiadam, by zainwestował w Nokię 3310. Telefony wychwytują bowiem nawet hasła kluczowe z naszych rozmów offline, podsłuchując nasze rozmowy. Zdaję sobie sprawę z tego, jak ogromne dane na temat naszego stylu życia, zainteresowań, pasji i pracy gromadzą popularne dzisiaj smartfony.

Jeśli nadal nie jesteście świadomi ogromu danych, które udostępniacie potentatom, czyli Google Inc (właściciel m.in. Gmail, YouTube, wyszukiwarka Google), Meta Social Metaverse Company (właściciel m.in. Instagrama, Facebooka, Messengera, WhatsApp), TikTok'owi i innym social mediom, to pokrótce postaram się to przedstawić. Praktyka prowadzenia szkoleń zamkniętych a także rozmów z przedsiębiorcami pokazuje mi, że to wciąż mało znany temat.

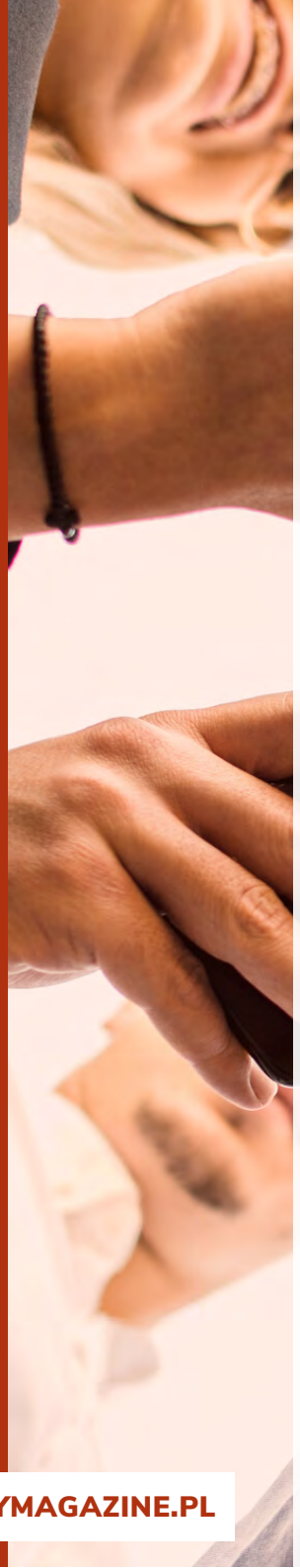
Nowoczesne smartfony pokochaliśmy, bo to małe komputery, które mieszczą się nam w kieszeni. Mamy na nich szereg aplikacji, które pozwalają nam komunikować się prywatnie i biznesowo. Mało kto zdaje sobie sprawę z tego, że jednocześnie to idealne narzędzia do szpiegowania. Przypomnę, że 80% osób z Internetu korzysta tylko przy pomocy przenośnych urządzeń typu smartfon. Jednocześnie nie dbamy o odpowiedniego antywirusa, otwieramy podejrzane linki, pobieramy różnego rodzaju aplikacje i oprogramowania.

Każda z aplikacji zainstalowanych na naszym smartfonie, w szczególności media społecznościowe, mają swoje kody szpiegujące, których zadaniem jest śledzić to, na jakie informacje reagujemy, które czytamy.

Tym sposobem tworzą wokół nas tzw. bańkę informacyjną. Docierają do nas tylko materiały, które wciągną nas w lekturę, sprawią, że spędzimy online więcej czasu. Najcenniejszą walutą jest tu właśnie czas i dane użytkowników.

JAKIE DANE ZBIERAJĄ MEDIA SPOŁECZNOŚCIOWE?

Popularne aplikacje, które instalujemy w swoich smartfonach to dla ich właścicieli kopalnia wiedzy na temat użytkowników.



W pierwszej kolejności zwrócę uwagę na to, że każdy link otwierany przez użytkownika Facebook'a i TikTok'a otwiera się w specjalnej przeglądarce wbudowanej w aplikację. Odczytuje ona nie tylko aktywność związaną z artykułem, ale i każde kolejne kliknięcie w inne linki.

Zbierane są także, co dla większości osób oczywiste, dane o naszych polubieniach, komentarzach, itp. Maszyny analizują także hasła, które padają w naszych konwersacjach na Messengerze i WhatsApp. Wszystko, by oferować nam reklamy, które najlepiej wpasowują się w nasz styl życia. Jeśli tylko w smartfonie uruchomimy lokalizację, to zczytują one także to, w jaki sposób poruszamy się po naszej miejscowości, kraju.

Ostatnio dużym echem odbił się artykuł opublikowany w amerykańskim magazynie Forbes. Pokazuje on, w jaki sposób aplikacja TikTok na co dzień zbiera informacje o swoich użytkownikach. Podobnie jak Facebook posiada ona specjalną, wbudowaną w nią przeglądarkę, przy pomocy której przeglądamy link otwierany w aplikacji. W taki sposób zbierane są wrażliwe dane na temat zainteresowań użytkowników. Wykorzystuje się do tego język programowania JavaScript.

Gwoli ciekawostki, naukowcy wskazują, że rzeczona przeglądarka TikTok'a posiada specjalny kod, który pozwala nie tylko monitorować, w jakie linki wchodzą użytkownicy. **Felix Krause, badacz aplikacji internetowych z Wiednia** wskazuje kilka prawidłowości.

Pokazuje, że w aplikacji zainstalowano tam również kod śledzący, jakie informacje wystukują weń użytkownicy przy pomocy klawiatury. Oczywiście, TikTok zaprzecza tym informacjom, twierdząc, że owszem, takie funkcjonalności kod ich aplikacji posiada, ale nie są one wykorzystywane w celu zbierania danych.

Krauze dowodzi, że kod jest wbudowany nie tylko w nowoczesny TikTok, ale i w narzędzia, które dostarcza firma Meta, właściciel Facebooka. Udowadnia on, że w obu przypadkach firmy faktycznie używają specjalnego kodu, który pozwala na zbieranie wrażliwych danych. Są one przechowywane na serwerach i udostępniane osobom trzecim.

Co interesujące, dokumenty polityki prywatności Facebooka oraz TikToka nie uwzględniają w danych takich informacji, jak aktywność przeglądarek w aplikacji mimo, że ujawniono praktyki monitorowania przez nie informacji czytanych przez użytkowników.

Wspomniany Krause wysłał do Apple oficjalne pytanie, czy nie może wymagać od aplikacji korzystania z domyślnej przeglądarki urządzenia, w tym przypadku Safari. Pozostało ono bez odpowiedzi.

Specjaliści z zakresu prywatności w Internecie ponadto sprzeciwiają się monitorowaniu kliknięć klawiszy klawiatury, o co posądzany został TikTok.

"Założenie, że twoje dane są wstępnie odczytywane, zanim je prześlesz dalej to przekroczenie granic" - mówi Jennifer King, specjalista ds. polityki prywatności i danych w Instytucie Sztucznej Inteligencji Skoncentrowanej na Człowieku Uniwersytetu Stanforda.

SZPIEGOSTWO PRZEMYSŁOWE W MEDIACH SPOŁECZNOŚCIOWYCH

Mało kto na co dzień mówi o ciemnej stronie prowadzenia mediów społecznościowych, także w ujęciu profesjonalnym.

Szeroko pojęty marketing w social mediach to nie tylko budowanie wizerunku marki, ale i sprzedawanie produktów, czy leadów. Do tego dodajmy także bieżący kontakt z klientami i budowanie relacji z nimi. Tak powstaje społeczność wokół marki. Szpiegostwo społecznościowe w ujęciu gospodarczym to próba uzyskania przewagi konkurencyjnej przy wsparciu wywiadu gospodarczego. Opiera się go na informacjach dostępnych w mediach społecznościowych. Co istotne, w takim ujęciu szpiegostwa bazujemy tylko na da-

nych publicznych - informacjach publikowanych przez konkretne marki w wielu kanałach komunikacji online. Nie jest to kradzież, ponieważ informacje te marki same publikują na swoich profilach.

Szpiegostwo społecznościowe w tym ujęciu polega na bacznym śledzeniu działań konkurencji, sprawdzaniu korespondencji, obserwacji dyskusji pomiędzy konkurencją a jej klientami.

DLACZEGO SZPIEGOSTWO SPOŁECZNOŚCIOWE ZYSKUJE NA ZNACZENIU?

Rewolucja technologiczna sprawia, że ogromna ilość firm jest obecna w mediach społecznościowych. Pandemia koronawirusa przyśpieszyła mechanizmy przenoszenia się wielu dziedzin życia do Internetu.

Efektem jest:

- bardzo szybki rozwój mediów społecznościowych,
- otwarcie firm na klientów i filozofia “need to share”,
- transformacja gospodarki wytwórczej w kierunku usługowej,
- zmiana trendów w obszarze wywiadu gospodarczego.

APLIKACJE SZPIEGOWSKIE W MEDIACH SPOŁECZNOŚCIOWYCH

Kolejnym aspektem są aplikacje szpiegowskie, które po instalacji w smartfonie pozwalają na szpiegowanie aktywności w wielu różnych mediach społecznościowych oraz najpopularniejszych komunikatorach: **WhatsApp, Messenger, Snapchat, Hangout.**

I choć wiele z nich powstało w dobrej wierze - by rodzice mogli kontrolować dzieci podczas ich aktywności online, wykorzystywane są one także do niecnych celów.

Jedną z marek szpiegowskich oferujących oprogramowanie szpiegowskie na smartfony jest TheOneSpy. Stworzyła ona kilkanaście różnych aplikacji szpiegowskich dla czatów w komunikatorach online. Korzystają z nich nie tylko rodzice, ale i pracodawcy, którzy chcą, by ich pracownik wykorzystywał w optymalny sposób czas pracy.

Dane użytkowników oraz firmowe publikacje to potężny oręż, który daje mediom społecznościowym możliwość sprzedaży spersonalizowanych reklam trafiających dokładnie do osób o wybranych zainteresowaniach.

Efekty reklam publikowanych na nich są niemalże natychmiastowe, a koszt reklamy dla przedsiębiorcy relatywnie niewielki. Stąd nadal przeciętny użytkownik mediów społecznościowych nadal może udzielać się w nich bezpłatnie.


/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

EDUKOWAĆ I UŚWIADAMIAĆ. CEL OSIĄGNIĘTY. PANCERNIK SECURITY SHOW

PATRONAT
SECURITY MAGAZINE

Promowanie najlepszych rozwiązań w zakresie bezpieczeństwa IT, edukacja, uświadamianie i wskazówki, jak bronić się przed cybernetycznymi atakami. Ogrom praktycznej, technicznej i przydatnej wiedzy w temacie cyberbezpieczeństwa - wszystko to, dostępne było w jednym miejscu – podczas szóstej edycji Pancernik Security Show.

Fot. Pancernik IT (2)

28 października w Katowicach odbyła się cyberbezpieczna konferencja **Pancernik Security Show**. Eksperci, którzy przeprowadzili 22 wykłady dla ponad 300 uczestników, przybliżyli im wiele aspektów i zagadnień, które po zastosowaniu, mogą podnieść poziom bezpieczeństwa ich firm i organizacji.

- Tematy prelekcji umożliwiły usystematyzowanie i zwiększenie swojej wiedzy – od procedur cyberbezpieczeństwa, poprzez zabezpieczenia danych i ochrony stron www i aplikacji, po monitoring infrastruktury i socjotechnikę - podsumowują organizatorzy.

GOŚCIE SPECJALNI

Podczas konferencji z cennymi wykładami wystąpili między innymi:

- **Dariusz Jakubowski Celber**, ekstrawagancki haker, hipster, z niepoważnym podejściem do życia – Niezależny Ekspert IT Security. Poprowadził lightning talk o historycznych metodach inwigilacji rodem z Podręcznika Anarchisty, które nadal znajdują swoje zastosowanie w XXI wieku. Wskazał rozwiązania „outside the box”, jak nie dać się złapać.

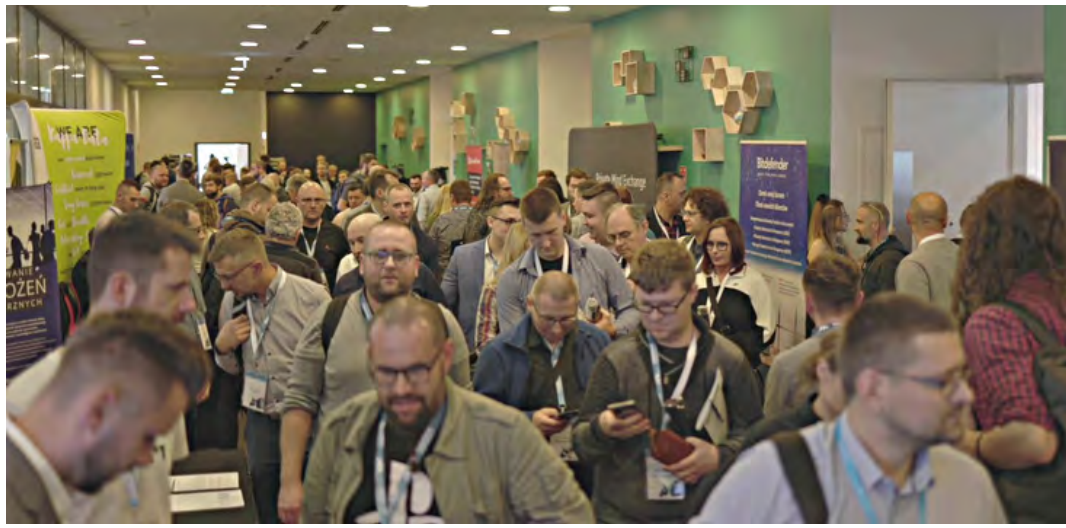
Fot. Pancernik IT (4)

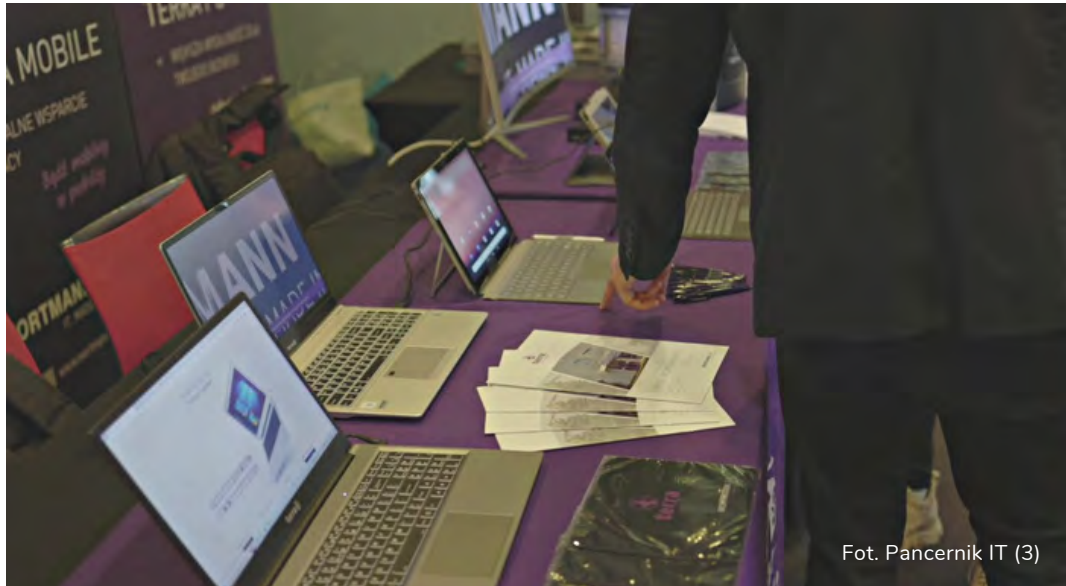
- **Adam Haertle** – uznany prelegent, trener i wykładowca – Redaktor Zaufana Trzecia Strona. Opowiedział, na co uważać dzisiaj i jutro – przegląd aktualnych zagrożeń.
- **Marcin Tynda** – Inspektor Ochrony Danych, trener oraz audytor wiodący ISO 27001, ekspert ECM i DMS przygotował prelekcję pod tytułem "Pentesterzy Offensive Security w akcji, czyli etyczne hackowanie: prezentacja na żywo jak się włamać i nie szkodzić."

ATAKI HAKERSKIE

Na konferencji była także możliwość wzięcia udziału w praktycznej stronie wydarzenia – warsztatach technicznych, podczas których można było nauczyć się konfiguracji backupu czy kompleksowej ochronie stacji roboczej i/lub serwera.

Ale Pancernik Security Show to nie tylko warsztaty oraz prelekcje, ale również kontrowersyjne pokazy hackingu przejmowania kontroli nad użytkownikiem itp. LABOR ZONE. Uczestnicy poznali mroczne hakerskie sekrety: jak pozyskać dane metodami socjotechnicznymi, jak znaleźć niezabezpieczone urządzenia IoT czy jak skopiować dane z kart. Wszystko po to, by wiedzieć, przed czym się bronić. Nie od dziś wiadomo, że by zwalczyć wroga, trzeba go najpierw poznać.





Fot. Pancernik IT (3)

Fot. Pancernik IT (4)

Fot. Pancernik IT (2)

DO WYBORU

W czasie konferencji uczestnicy mieli do wyboru masę wystąpień, w tym “Widoczność, Kontrola, Analityka w kolejnych warstwach ochrony”, “Procedura cyberbezpieczeństwa – checklista w stanach alarmowych”, “Wektory ataku a inteligentne rozwiązania SOC”, “Antywirus oraz it manager z poziomu jednej konsoli”, “Dlaczego dostęp do danych jest tak ważny?”, “Wykorzystanie Chmury w cyberbezpieczeństwie – Święty Graal czy przekleństwo?”, “Passwordless czy hasło, co przyniesie przyszłość?”, “Socjotechnika z zaplecza”, “Monitoring pracowników i firm trzecich. Jak robić to dobrze i zgodnie z prawem?”, “Jak skutecznie chronić strony internetowe i aplikacje przed atakami?” oraz wiele innych.

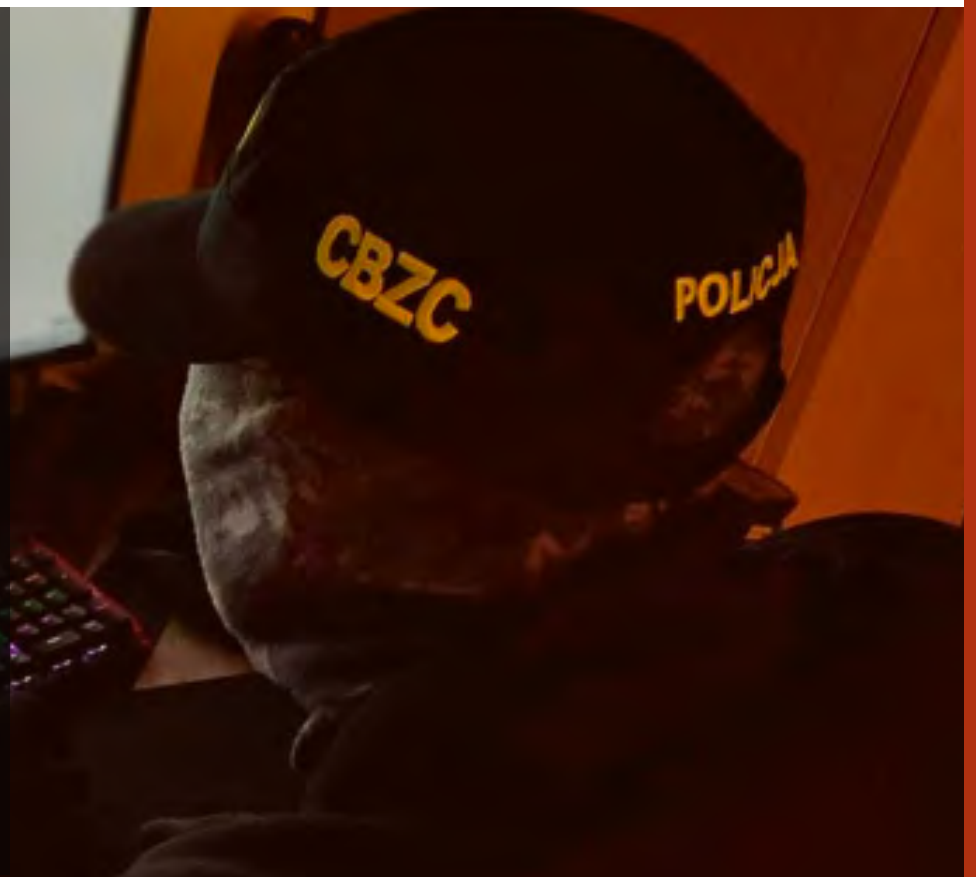
Pancernik Security Show to połączenie dawki wiedzy z elementami rozrywki. Była Strefa Gier Retro i konkursy.

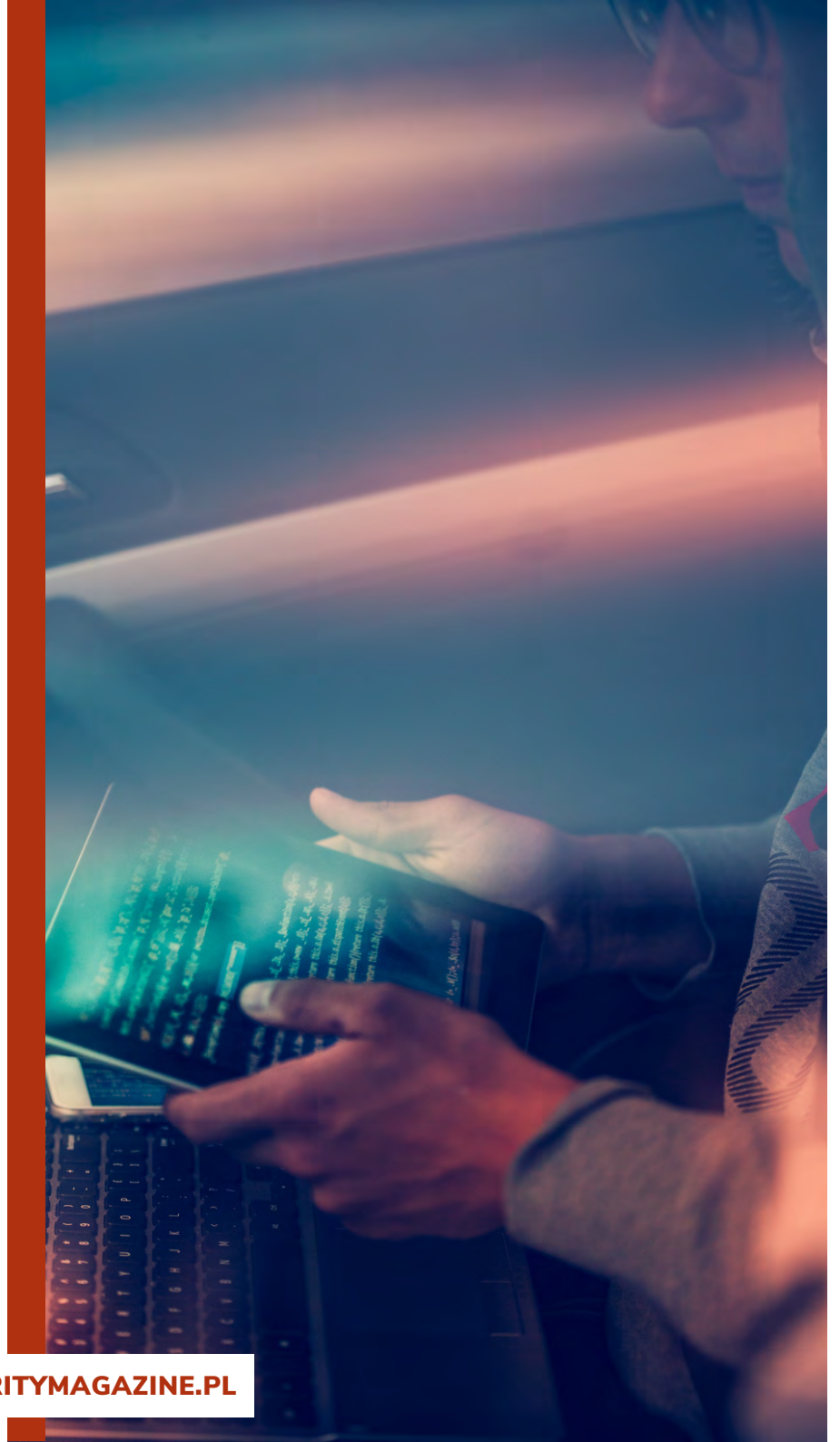

Organizujesz wydarzenie związane
z bezpieczeństwem w firmie
lub nowymi technologiami?
Sprawdź ofertę
PATRONATU
MEDIALNEGO
SECURITY MAGAZINE
Napisz do nas:
redakcja@securitymagazine.pl

CYBERPOLICJA VS. CYBERPRZESTĘPCY

podkom. Marcin Zagórski
Centralne Biuro Zwalczania Cyberprzestępczości

Każdy, kto posiada lub zarządza cennymi aktywami, cyfrowymi lub materialnymi i chce umożliwić dostęp do nich innym, nawet, jeśli jest to niewielka grupa ludzi, zadaje sobie pytanie: w jaki sposób mogę zapewnić, że te aktywa nie trafią w złe ręce? To wtedy musimy zdać sobie sprawę, że urządzenia lub oprogramowanie nie popełniają przestępstw, ale ludzie to robią.





CYBERPOLICJA I JEJ CELE

Zwalczanie cyberprzestępczości powinno się opierać na ograniczaniu skutków jej wpływu na społeczeństwo oraz identyfikowaniu zagrożeń pochodzących z sieci, a co za tym idzie na tworzeniu bezpieczniejszej cyberprzestrzeni.

Taki jest cel Centralnego Biura Zwalczania Cyberprzestępczości (CBZC), które jest jednostką organizacyjną Policji. CBZC odpowiedzialne jest za realizację na obszarze całego kraju zadań w zakresie:

- rozpoznawania i zwalczania przestępstw popełnionych przy użyciu systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej i zapobiegania tym przestępstwom, również wykrywania i ścigania sprawców tych przestępstw;
- wspierania w niezbędnym zakresie jednostek organizacyjnych Policji w rozpoznawaniu, zapobieganiu i zwalczaniu tych przestępstw.

Centralnym Biurem Zwalczania Cyberprzestępczości kieruje Komendant Centralnego Biura Zwalczania Cyberprzestępczości, który podlega Komendantowi Głównemu Policji.

CZYNY PRZESTĘPCZE

Komisja Wspólnot Europejskich definiuje cyberprzestępczość jako czyny przestępcze dokonane przy użyciu sieci łączności elektronicznej i systemów informatycznych lub skierowane przeciwko takim sieciom i systemom, która przejawia się w trzech formach:

1. **Tradycyjne formy** działalności przestępczej (oszustwa, phishing itp.)
2. **Publikacja nielegalnych treści** (np. materiały nakłaniające do terroryzmu, przemocy czy seksualnego wykorzystania dzieci)
3. **Przestępstwa typowe dla sieci** łączności elektronicznej (czyny o dużym zasięgu i na masową skalę, które przed pojawieniem się internetu nie miały miejsca).

Generalnie można przyjąć, że przestępstwa cyber to takie, do popełnienia których konieczne jest użycie sieci informatycznej lub teleinformatycznej.

Ostatnie lata wyraźnie wskazują na wzrost czynów popełnionych w cyberprzestrzeni.

HAKER? PRZESTĘPCA

Centralne Biuro Zwalczania Cyberprzestępczości w swoich działaniach nie używa pojęcia haker, nie jest to określenie ustawowe. Skupiamy się na czynach i przestępstwach popełnionych w sieci, wykryciu sprawców tych przestępstw i postawieniu ich przed sądem.

Jeśli chodzi o proces wykrywczy cyberprzestępstw, to trzeba wskazać, że działania te wymagają użycia specjalistycznego sprzętu czy oprogramowania.

Takimi narzędziami dysponują funkcjonariusze CBZC, jednak jest to proces wymagający dużego nakładu czasu. Funkcjonariusze Biura przede wszystkim w początkowym okresie jego funkcjonowania skupiają się na dużych, najpoważniejszych sprawach. Przeprowadzili już kilkanaście realizacji na terenie całego kraju.

Zatrzymaliśmy blisko 30 osób, z których wobec 18 zastosowano środki zapobiegawcze w postaci tymczasowego aresztowania, w różnych kategoriach przestępstw: głównie oszustwa, ale również wykorzystywanie seksualne dzieci i rozpowszechnianie takich materiałów w sieci, czy fałszowanie certyfikatów „covidowych".

W swoich działaniach staramy się zachęcać wszystkich, którzy stali się celem cyberataku, aby każdą informację przekazywać policjantom. Można to zrobić na wiele sposobów i w każdej jednostce Policji w kraju. Takie podejście powoduje, że odbieramy przestępcom ich główny motyw – szantaż finansowy.

Zagrożenie karą za przestępstwo popełnione w cyberprzestrzeni zależy, oczywiście, od rodzaju tego przestępstwa.

Najsurowiej karane są przestępstwa z kategorii publicznego prezentowania treści pornograficznych np. produkcja, utrwalanie lub sprowadzanie, przechowywanie lub posiadanie albo rozpowszechnianie treści pornograficznych z udziałem małoletniego zagrożone jest karą nawet do 12 lat pozbawienia wolności.

Czyny te, są jednym z priorytetowych kierunków walki z cyberzagrożeniami dla funkcjonariuszy Centralnego Biura Zwalczania Cyberprzestępczości.

Natomiast istotnym elementem odstraszającym potencjalnych przestępców od popełnienia danego czynu jest przede wszystkim świadomość o skuteczności organów ścigania oraz nieuchronności wymierzonej kary."

BEZPIECZEŃSTWO PRAWNE MEDYKÓW. JAK JE OSIĄGNĄĆ?

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

Bezpieczeństwo jest jedną z podstawowych potrzeb każdego człowieka – i to właściwie na każdej płaszczyźnie jego funkcjonowania. Przeciwdziałanie występowaniu wypadku przy pracy to za mało – zwłaszcza w zawodach, których wykonywanie obciążone jest dużym ryzykiem popełnienia błędu mogącego doprowadzić nawet do utraty zdrowia i życia.

Bez wątpienia zawody medyczne mieszczą się w tej grupie, a zapewnienie bezpieczeństwa – zwłaszcza prawnego, dotyczącego przede wszystkim sfery odpowiedzialności za błędy w sztuce – medyków ma bezpośrednie przełożenie na jakość systemu ochrony zdrowia.

Podstawowym problem sprowadza się do pytania o zasady, na podstawie których medyk powinien odpowiadać za swoje błędy.

CZYM JEST BEZPIECZEŃSTWO PRAWNE?

W najbardziej podstawowym znaczeniu bezpieczeństwo jest definiowane, jako stan braku zagrożenia, spokoju dający poczucie pewności oraz stwarzający poczucie realnej ochrony przed różnego rodzaju niebezpieczeństwami. Tym samym „bezpieczeństwo" jest niezwykle szeroką kategorią, którą można odnieść zarówno do funkcjonowania jednostki, jak i całych społeczeństw i państw, a nawet wspólnoty międzynarodowej.

W tym kontekście mówi się o bezpieczeństwie publicznym i prywatnym czy bezpieczeństwie zdrowotnym, ekonomicznym, oświatowym, ekologicznym, narodowym, powszechnym itp.

O bezpieczeństwie na każdej z tych płaszczyzn można mówić w specyficznym znaczeniu, jednak ich wspólnym mianownikiem jest potrzeba eliminowania zagrożeń.

Coraz częściej zwraca się uwagę na problem bezpieczeństwa prawnego. W literaturze prawniczej – zarówno polskiej, jak i zagranicznej – jest ono rozmaicie ujmowane.

Najczęściej wskazuje się, że przez bezpieczeństwo prawne należy rozumieć stan, w którym podstawowe interesy i uprawnienia człowieka bądź innego prawa są odpowiednio chronione w sposób całkowity i skuteczny. Drogą do osiągnięcia bezpieczeństwa prawnego jest system prawa pozytywnego, a więc – mówiąc w pewnym uproszczeniu – zbiór przepisów prawnych.

Bezpieczeństwo prawne nie jest jedynie abstrakcyjną ideą, ale – co pokazuje chociażby orzecznictwo sądów konstytucyjnych, w tym polskiego Trybunału Konstytucyjnego – pociąga za sobą szereg różnego rodzaju konsekwencji. Kiedy realizuje się postulaty wypływające z idei bezpieczeństwa prawnego, to każdy adresat regulacji prawnych wie, jak ma postępować – czyli co jest mu nakazane, co

zabronione – oraz może zaplanować swoje działania, gdyż wie, że nie będzie zaskoczony zmianami prawa, które uniemożliwią lub znacznie utrudnią mu realizację jego zamierzeń. Dlatego bezpieczeństwo prawne jest możliwe tylko wówczas, gdy przepisy prawa są jasne, przejrzyste, nie zmieniają się zbyt często, a praktyka ich stosowania jest utrwalona.

MEDYK W SKOMPLIKOWANYM SYSTEMIE

Każdy, kto miał do czynienia z polskim prawem wie, jak daleko mu do tych ideałów. To z kolei przekłada się na wysoki poziom „niebezpieczeństwa prawnego", zwłaszcza w stosunku do osób podejmujących skomplikowane zadania, obciążone dużą dozą ryzyka i odpowiedzialności związanej z ewentualnymi błędami i niepowodzeniami.

W grupie tej z pewnością mieszczą się wszyscy wykonujący zawody medyczne. Jaki więc kształt powinny przybrać unormowania prawa medycznego, aby spełniały standardy bezpieczeństwa prawnego? Przede wszystkim należy pamiętać, że praktycznie każdy medyk może ponieść zarówno odpowiedzialność karno- i cywilnoprawną, jak i dyscyplinarną, wobec organów samorządu zawodowego.

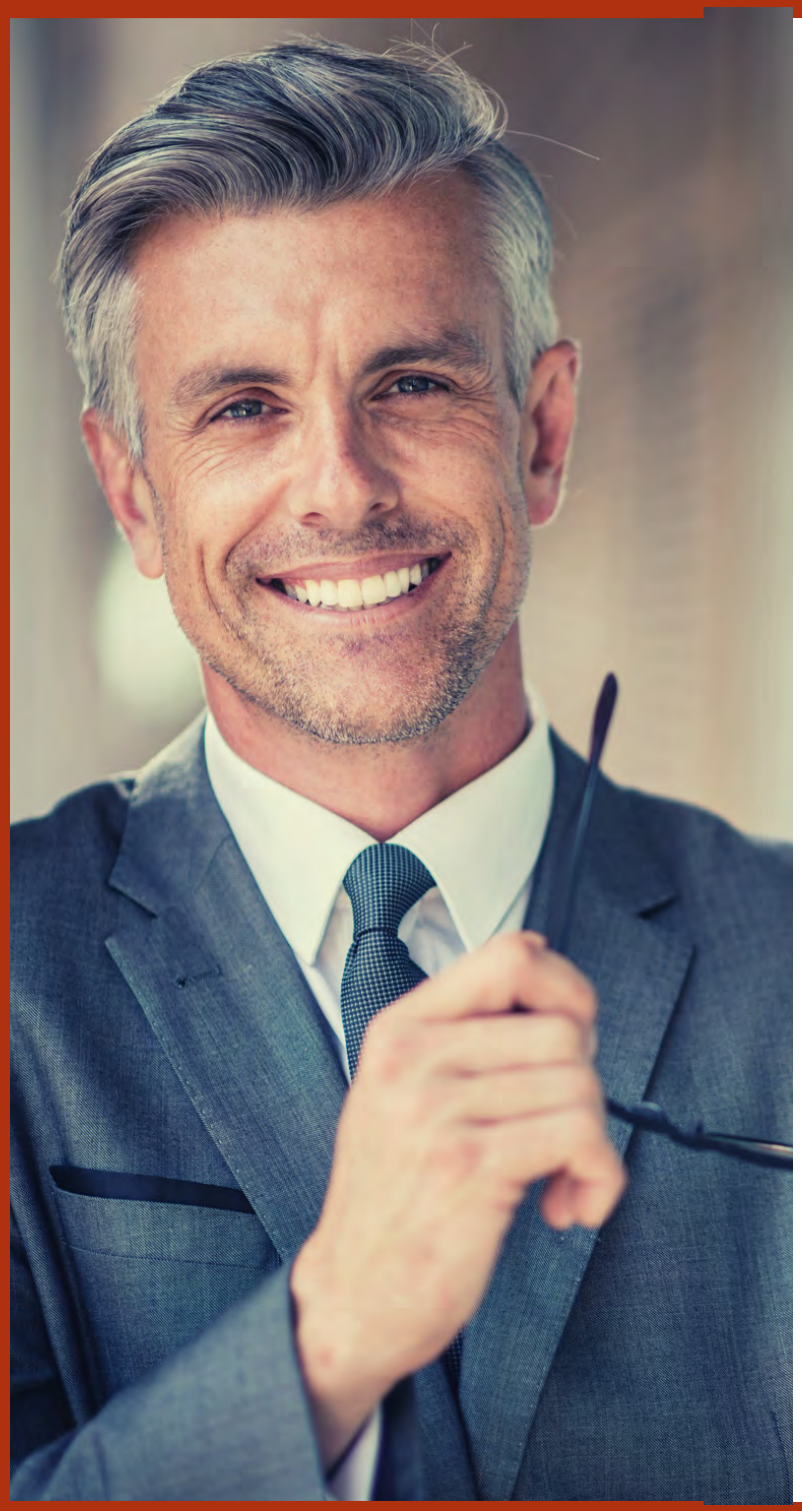
Na te uwarunkowania nakłada się konieczność pracy w skomplikowanym – i niestety niezbyt dobrze zorganizowanym – systemie ochrony zdrowia, który jest w stanie zagwarantować prawidłową opiekę nad pacjentem tylko wówczas, gdy dobrze działa, jako całość.

Pojedynczy medyk w istocie niewiele może, tymczasem zawsze ponosi indywidualną odpowiedzialność. Zarówno prawidłowa, jak i błędna opieka nad pacjentem rzadko kiedy jest wynikiem jednostkowych decyzji, przeważnie stanowiąc rezultat całego ciągu zdarzeń. Z tego względu nie sposób nie uwzględnić tych uwarunkowań przy określaniu zasad odpowiedzialności za błędy w sztuce.

W tym kontekście warto zwrócić uwagę na problem wprowadzenia systemu no-fault, który zakłada rezygnację z możliwości orzekania o odpowiedzialności karnej za popełnienie (nieumyślnego) błędu w sztuce medycznej, przy jednoczesnym zagwarantowaniu prawa pacjenta do uzyskania rekompensaty. W systemie odpowiedzialności opartej na założeniach no-fault nacisk kładzie się nie tyle na winę indywidualnego medyka, ale na wykrycie i wyeliminowanie przyczyn, które doprowadziły do błędu skutkującego szkodą oraz krzywdą pacjenta. Dlatego nie bez racji system ten porównuje się do badania wypadków lotniczych.

BEZPIECZEŃSTWO MEDYKA I PACJENTA

Celem istnienia ochrony zdrowia jest pacjent. Jednak jego prawidłowe leczenie i opiekę można zapewnić tylko wówczas, gdy posiada się odpowiednio wykwalifikowany personel, mający poczucie własnego bezpieczeństwa – także prawnego. Tymczasem aktualny system odpowiedzialności za niepożądane zdarzenia medyczne służy raczej typowej „spychologii", niż rzeczywistemu podnoszeniu standardów opieki oraz rekompensowaniu negatywnych skutków błędów, które dotykają pacjentów będących ich ofiarami. Tym samym jego zmiana może przyczynić się do poprawy jakości opieki zdrowotnej. Na tym zaś powinno zależeć nam wszystkim. W końcu każdy z nas jest potencjalnym pacjentem.



DOŁĄCZ DO GRONA EKSPERTÓW

BUDUJ SWOJĄ MARKĘ
I ROZPOZNAWALNOŚĆ
SWOJEJ FIRMY

SECURITY MAGAZINE

WWW.SECURITYMAGAZINE.PL

EKSPERCI WYDANIA

MACIEJ PAWLAK
Head of Risk & Security
Tpay

W Tpay odpowiedzialny za zarządzanie ryzykiem i bezpieczeństwo informacji. Od ponad 10 lat związany z branżą fintech. Ekspert w dziedzinie compliance oraz zarządzania ryzykiem niezgodności w instytucjach regulowanych. Współodpowiedzialny za proces uzyskiwania licencji instytucji płatniczej dla pierwszego kantoru internetowego w Polsce.

BEATA ŁASZYN
Wiceprezeska
Alert Media Communications

Ekspertka komunikacji kryzysowej – począwszy od przygotowania do kryzysów, przez wsparcie w komunikacji, na audytach pokryzysowych kończąc. Wykonuje analizy, opracowuje strategie komunikacji. Współautorka poradnika „e-Kryzys. Jak Zarządzać Sytuacją Kryzysową w Internecie" Wiceprezeska Alert Media Communications.

INSP. DR MARIUSZ CIARKA
Rzecznik Prasowy
Komenda Główna Policji

Oficer Policji w stopniu inspektora, doktor nauk prawnych, od 2016 roku rzecznik prasowy Komendanta Głównego Policji. Członek Prezydium Rady Polityki Penitencjarnej III kadencji na lata 2020–2024. Dyrektor Biura Komunikacji Społecznej Komendy Głównej Policji. Redaktor naczelny Gazety Policyjnej i miesięcznika POLICJA997.

RAFAŁ LACHOWICZ
Specjalista ds. zapobiegania i wykrywania przestępstw gospodarczych i korupcji

Kierownik Działu Kontroli oraz Koordynator ds. Nadużyć Finansowych w Urzędzie Marszałkowskim Województwa Dolnośląskiego. Certyfikowany specjalista ds. zapobiegania i wykrywania przestępstw gospodarczych i korupcji. Specjalizuje się w obszarze przeciwdziałania i wykrywania nadużyć finansowych.

EKSPERCI WYDANIA

MARCIN ZAGÓRSKI
podkomisarz
Centralne Biuro Zwalczania Cyberprzestępczości

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

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 CHOLEWCZYŃSKI
Broker
Infinity Brokerzy Ubezpieczeniowi Sp. z o.o.

Broker z wieloletnim doświadczeniem w likwidacji szkód i ocenie ryzyka ubezpieczeniowego. Obecnie odpowiedzialny za obsługę klientów z branży IT, w szczególności w zakresie ubezpieczeń OC zawodowych dla spółek tworzących oprogramowanie. Wspiera klientów w znalezieniu ubezpieczenia zgodnego z ich realnymi potrzebami i wymaganiami.

KONRAD DYDA
Prezes Zarządu
Med&Lex-Klinika 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 - Klinika Wsparcia Personelu i Jednostek Ochrony Zdrowia oraz w Fundacji Praw Medyka.

PARTNERZY WYDANIA

KOMENDA GŁÓWNA POLICJI

PUBLITO.PL

SERWIS ŁĄCZĄCY EKSPERTÓW
Z DZIENNIKARZAMI

POLITYKA BEZPIECZEŃSTWA

SERWIS INFORMACJNY
O BEZPIECZEŃSTWIE FIRM

RZETELNY REGULAMIN

BLOG POŚWIĘCONY
POLSKIEMU E-COMMERCE

POLICJA

publito

Polityka® Bezpieczeństwa

Rzetelny® Regulamin

SECURITYMAGAZINE.PL

ZOBACZ WYDANIA

Wydanie 1/2022

POBIERZ

Wydanie 2/2022

POBIERZ

Wydanie 3/2022

POBIERZ

Wydanie 4/2022

POBIERZ

Wydanie 5/2022

POBIERZ

Wydanie 6/2022

POBIERZ

Wydanie 7/2022

POBIERZ

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, skład i korekta: Monika Świetlińska

Współpraca i kontakt: redakcja@securitymagazine.pl

SECURITYMAGAZINE.PL