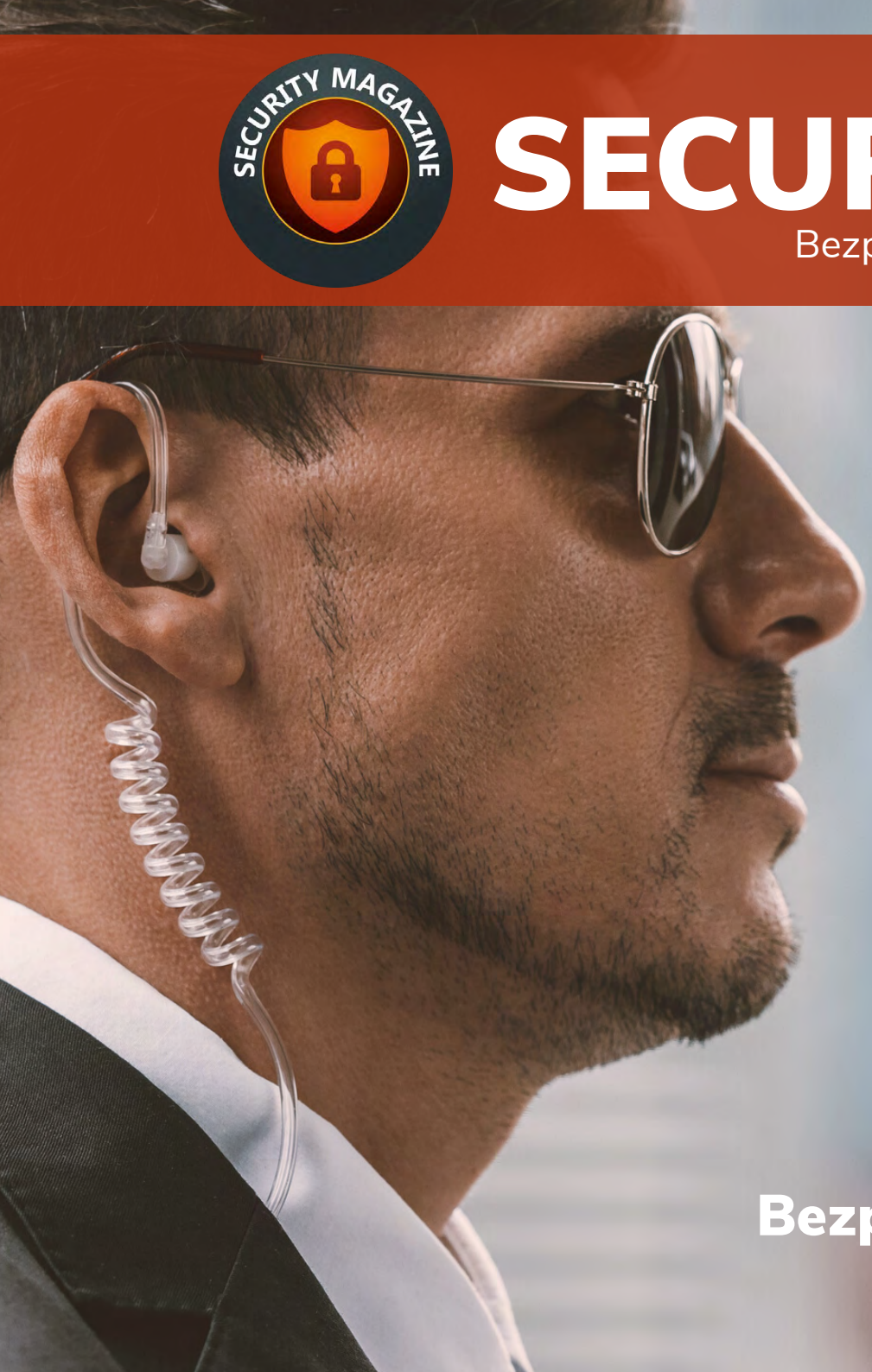
06/2022

SECURITY MAGAZINE

Bezpieczeństwo | Technologia | Wiedza | Najlepsze standardy



Czego możesz wymagać od firmy ochroniarskiej?

System kontroli dostępu drzwi Jak wybrać?

Kategoryzacja alertów AI może to zrobić za Ciebie!

Pięć trudnych lat z ransomware Jak przechytrzyć cybergangi?

Bezpieczeństwo przechowywania danych w systemie CRM oraz ERP w chmurze

SPIS TREŚCI

SZANOWNI PAŃSTWO,

"Security Magazine" rozwija się z miesiąca na miesiąc. Jest nam miło przekazać Wam trzy ważne informacje.

Pierwsza jest taka, że nasze dotychczasowe wydania, a było ich pięć, trafiły już do ponad 100 tys. czytelników, z czego ostatnie - wydanie wakacyjne - mimo sezonu urlopowego zanotowało najwyższą liczbę pobrań. To pokazało nam, że po "Security Magazine" sięgacie coraz chętniej.

Druga - startujemy z cyklem "Security Startup". Nasz redaktor, który na start up-ach zna się, jak mało kto, co miesiąc prezentował będzie kilka polskich i zagranicznych rozwiązań mogących w znacznym stopniu wpłynąć na bezpieczeństwo w Waszych firmach.

Trzecia - nawiązaliśmy owocny kontakt z Komendą Główną Policji, z którą będziemy współtworzyć rubrykę dla przedsiębiorstw dotyczącą ich bezpieczeństwa. Pierwsze efekty już na łamach tego wydania.

Zapraszam do lektury.

Rafał Stępniewski

ZAPISZ SIĘ

NA

NEWSLETTER

BY NIE PRZEOCZYĆ
KOLEJNEGO WYDANIA

SECURITY MAGAZINE

SOCJOTECHNIKI PRZESTĘPCÓW CIĄGLE SKUTECZNE

Dariusz Polaczyk
Currency One SA

Mimo licznych kampanii informacyjnych nadal słyszymy o kolejnych ofiarach oszustów grasujących w sieci lub działających za pomocą telefonu. Według Policji, kwoty wyłudzeń można liczyć w milionach złotych, a bardzo często oszukani tracą oszczędności swojego życia. Atakowani są przede wszystkim seniorzy, choć odnotowywane są również przypadki oszukania ludzi młodych.

Niestety, inwencja przestępców jest nieograniczona, musimy więc być bardzo czujni, by z uczestnika pozornie niewinnej i pozbawionej ryzyka sytuacji nie stać się ofiarą dużego oszustwa.

Mechanizmów wyłudzeń jest bardzo wiele, trudno wymienić wszystkie, spróbuję więc je skatalogować:

NIEPOKOJĄCE SMS-Y LUB E-MAILE

które grożą rzekomo niezapłaconą fakturą, egzekucją komorniczą, pozwem sądowym, wpisem do rejestru długów itp. Celem jest wywołanie strachu, obawy i chęci najszybszego poznania szczegółów,

„NA POLICJANTA”

dzwoni osoba podszywająca się pod policjanta i informuje nas, że ktoś włamał się na nasze konto bankowe i za chwilę nas okradnie, jeżeli nie zabezpieczymy swoich środków. Potencjalna ofiara proszona jest o udanie się do banku, wypłacenie wszystkich środków ze swojego konta i pozostawienie ich w umówionym miejscu. Jeżeli oszust zorientuje się, że ta obsługuje swój rachunek przez internet, to proszona jest o wykonanie przelewu na „bezpieczne, tymczasowe konto”.

„NA PREZESA”

otrzymujemy maila lub telefon, rzekomo od prezesa naszej firmy, z prośbą czy poleceniem wykonania operacji finansowej.

FAŁSZYWE INWESTYCJE

w popularnych serwisach społecznościowych oszuści zamieszczają reklamy zachęcające do inwestowania w obligacje państwowych spółek z branż energetyczno-paliwowych. Często towarzyszy im wizerunek znanych polityków albo celebrytów rzekomo wspierających tę inicjatywę. Co zdumiewa, to fakt, że portale te tak łatwo zgadzają się na zamieszczanie oszukańczych reklam – po ostatniej głośnej fuzji na rynku paliwowym w Polsce nastąpił „wysyp” tego typu „ofert”. W innych wariantach oszuści zachęcają do lokowania środków w kryptowalutach, podając się za młodą, atrakcyjną osobę, która rzekomo sama to zrobiła i teraz korzysta z życia, poświęcając inwestycji kilkanaście minut dziennie. Co najgorsze, ofiary często same kontaktują się z oszustami po przeczytaniu reklam, zachęcone ich treścią. Wysoka inflacja, połączona z nienadążającym za nią oprocentowaniem lokat bankowych, powoduje, że ludzie szukają innych form ratowania swoich oszczędności, a oszuści zręcz-

nie to wykorzystują. Ofiary same przelewają im swoje środki lub też pozwalają – przekonane, że korzystają z pomocy technicznej – na instalację na swoim komputerze lub telefonie tzw. zdalnego pulpitu, co umożliwia przestępcom przejęcie całkowitej kontroli nad urządzeniem.

SZKODLIWE ZAŁĄCZNIKI LUB LINKI W E-MAILACH

treść maila ma albo zachęcić nas do otwarcia załącznika (klasyczny przykład: w załączeniu „Pozew sądowy"), albo też „ukryć się" w masie podobnych wiadomości (przykład: przesłanie faktury do biura rachunkowości lub CV do agencji rekrutacyjnej). Otwarcie załącznika lub wejście w link może wiązać się z instalacją szkodliwego oprogramowania, czego skutkiem może być kradzież wrażliwych danych, zaszyfrowanie dysku w celu wyłudzenia okupu za odkodowanie znajdujących się na nim plików, śledzenie naszej aktywności w sieci itd.

OSZUSTWA NIGERYJSKIE

informacja o spadku, wielkiej nagrodzie, wygranej na loterii albo, w innej odsłonie próby rozkochania przez amerykańskich generałów czy pułkowników, bogatych i samotnych biznesmenów itd.

Może wydawać się to niebywałe, ale, niestety, tak jest, że ludzie są w stanie uwierzyć i przekazać pieniądze w wysokości nawet kilkudziesięciu tysięcy złotych osobie, której nigdy w życiu nie spotkali osobiście. Przy nagrodach i spadkach oszuści chcą namówić nas do wysłania mniejszej kwoty celem uzyskania większej (potrzeba opłacenia podatku, kosztów sądowych itp.).

OSZUSTWA WAKACYJNE

oferta atrakcyjnego pobytu wakacyjnego w obiekcie, którego nie ma lub który nie należy do osoby sprzedającej pobyt.
Dodatkowo można zapłacić za fałszywy wynajem samochodu, lot czy podróż pociągiem, czarter łodzi itp.

Socjotechniki przestępców ciągle skuteczne

FAŁSZYWE ZBIÓRKI

wojna w Ukrainie, pandemia, katastrofy, wypadki czy choroby uruchamiają w ludziach chęć niesienia pomocy. Oszuści wykorzystują to, zamieszczając informację o fałszywych zbiórkach.

OSZUSTWA ZAKUPOWE

kupujemy w sieci nieistniejący towar lub usługę, za które płacimy z góry. Gdy z kolei coś sprzedajemy, przestępca podszywający się pod kupującego może dążyć do wyłudzenia danych karty płatniczej w celu rzekomego przelania na nią środków.

POTWIERDZANIE NASZEJ TOŻSAMOŚCI

pod pozorem konieczności potwierdzenia naszej tożsamości oszuści podstawiają nam fałszywą stronę portalu społecznościowego, banku lub innej instytucji, gdzie podajemy dane logowania lub inne dane wrażliwe, które mogą później wykorzystać, np. do wykradzenia środków z naszego konta bądź zaciągnięcia na nas pożyczki.

ATAKI SPERSONALIZOWANE

jedne z najniebezpieczniejszych. Czekamy na paczkę i właśnie wtedy przychodzi SMS o konieczności dopłaty za jej dostarczenie przez kuriera albo otrzymujemy wiadomość o potrzebie uregulowania należności akurat w momencie, gdy zrobiliśmy zakupy. Oszust wplata się w naszą realną sytuację i informacja z tym związana nie wzbudza naszych podejrzeń. W ostatnim czasie odnotowano przypadek, w którym oszuści spisywali podawane głośno dane osoby wygrywającej licytację. Następnie osoba ta otrzymała informację o danych do przelewu za wygraną licytację. Alternatywna forma to masowa wysyłka SMS czy e-maili podszywających się pod największe banki, czy inne instytucje. Oszuści po prostu liczą na to, że przypadkowy odbiorca takiej wiadomości okaże się jednym z klientów tych instytucji. Jeszcze inny możliwy schemat to powiadamianie o zmianie numeru rachunku bankowego służącego do przyjmowania opłat za gaz, energię, usługi itp.

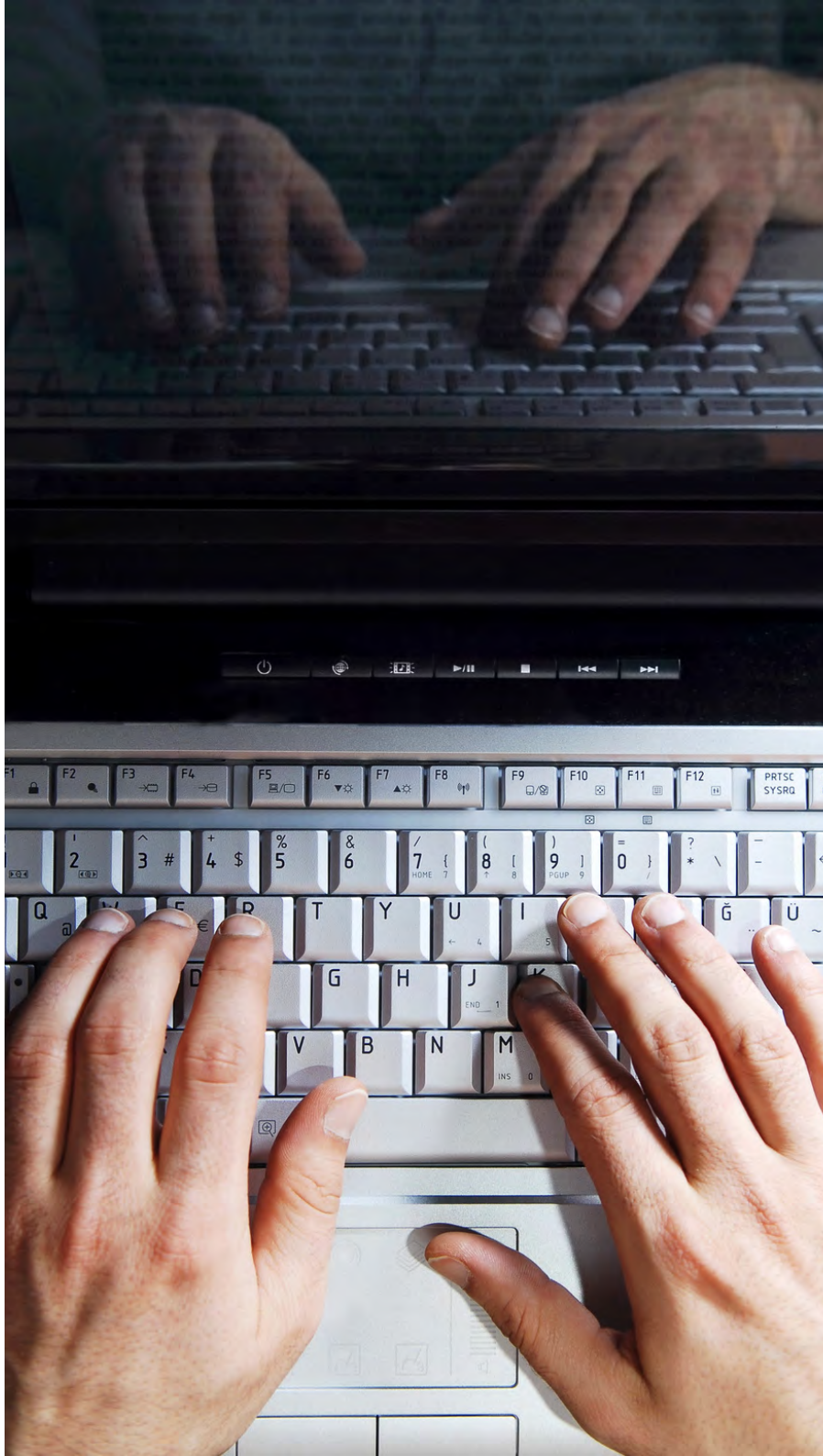
WYCIEK DANYCH DOSTĘPOWYCH

zdarza się, że nasze dane dostępowe zostają przejęte przez oszustów w wyniku wycieku ze słabo zabezpieczonego portalu. Jeżeli przestrzegamy zasady unikatowości hasła, czyli do każdego serwisu logujemy się innym ciągiem znaków, a dodatkowo tam, gdzie to możliwe, włączamy podwójne uwierzytelnienie, to poza skompromitowanym serwisem jesteśmy bezpieczni. Problem pojawi się w momencie, gdy używamy tego samego hasła do różnych serwisów i nie stosujemy podwójnego uwierzytelnienia. Przejęcia większości kont na portalach społecznościowych czy sprzedażowych mają właśnie taką genezę.

CO POWINNO BYĆ SYGNAŁEM OSTRZEGAWCZYM?

Pomimo że scenariusze oszustw są zmienne i dostosowane do aktualnej sytuacji, to można znaleźć w nich stałe elementy, których obecność powinna być dla nas dzwonkiem alarmowym. Przede wszystkim oszuści bazują na naszych emocjach, dążą do wywołania pośpiechu, strachu, zaciekawienia, chęci natychmiastowego sprawdzenia otrzymanej informacji.

Dlatego uważajmy, gdy w komunikacji pojawiają się przynajmniej niektóre z tych charakterystycznych elementów:



- groźba, straszenie karą, grzywną, kompromitacją, sprawą sądową, ujawnieniem naszych osobistych sekretów itp.;
- nacisk na natychmiastowe działanie (superpromocja, która za chwilę się skończy, nagranie będzie dostępne jeszcze 15 minut, okazja dla pierwszych 50 klientów, tylko dzisiaj itp.);
- nietypowa prośba (najczęściej finansowa) mogąca pochodzić również od znajomego (oszust podszywa się pod niego);
- podejrzany link lub załącznik;
- błędy językowe - coraz rzadsze, ale jeśli występują (szczególnie w komunikatach od szanowanych instytucji), są silnym sygnałem ostrzegawczym. Choć błędy ortograficzne, gramatyczne, składniowe mogą przytrafić się każdemu, to jednak bardzo mało prawdopodobne, by trafiły do np. oficjalnego komunikatu czy zawiadomienia;
- brak polskich liter (nie dotyczy SMS) - w oficjalnej komunikacji e-mailowej instytucja nie pozwoli sobie na takie uproszczenie;
- język potoczny lub nadmiernie urzędowy;
- niska jakość grafik;
- domena, z której przysłano e-mail, inna niż oficjalna;
- rzekomy klient portalu zakupowego kontaktuje się z nami lub chce przeprowadzić płatność innymi sposobami niż te udostępniane przez taki portal;
- brak adresu firmy lub wskazanie skrytki pocztowej;
- brak informacji o firmie w internecie.

Generalna zasada mówi, że jeśli cokolwiek wzbudza nasze podejrzenie, obawę, nawet gdy czasami trudno określić co konkretnie, to powinniśmy wstrzymać się z działaniem, poczekać chwilę, zastanowić się. Celem oszustów jest spowodowanie, żebyśmy działali impulsywnie, bezrefleksyjnie, natychmiastowo. Nie pozwólmy im na to.

PATRONAT
SECURITY MAGAZINE

Kongres Profesjonalistów
Public Relations

Zgłoś się na
Kongres PR w Rzeszowie
już dziś!

Zapisy trwają!

Rzeszów,
15-16 września 2022

www.**kongrespr**.pl

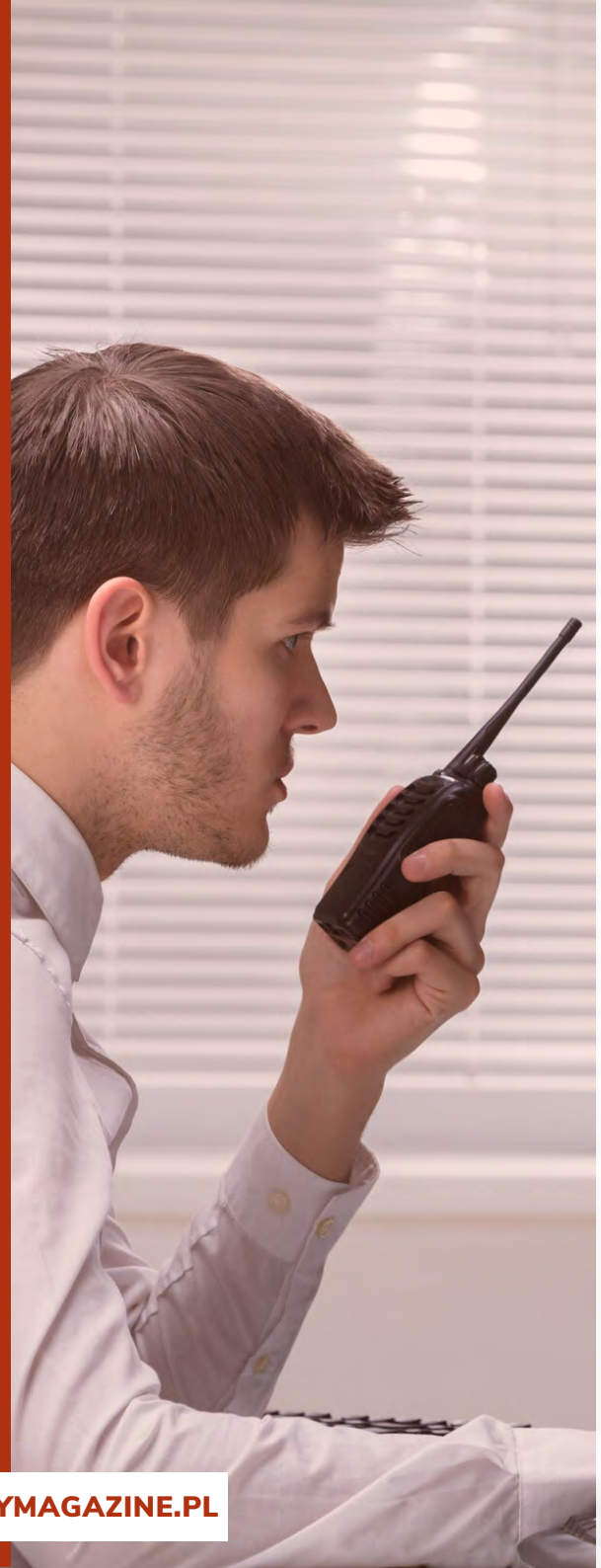
#Kongres**PR2022**

SECURITYMAGAZINE.PL

CZEGO MOŻESZ WYMAGAĆ OD FIRMY OCHRONIARSKIEJ?

Redakcja
SECURITY MAGAZINE

Bezpieczeństwo to nie tylko kwestia cyfrowa, ale też fizyczna. Toteż zatrudniając agencję ochroniarską, warto wiedzieć, czego możesz od niej wymagać i na co musisz zwrócić uwagę przy jej wyborze. W tym tekście odpowiemy na pytanie, co charakteryzuje dobrą firmę ochroniarską.



JAK ZWERYFIKOWAĆ BIURO OCHRONY?

Centralny Ośrodek Informacji Gospodarczej dysponuje listą 3647 agencji ochrony w Polsce. A i tak prawdopodobnie nie są to wszystkie podmioty. Te największe zatrudniają nawet kilka czy kilkadziesiąt osób i pracują dla największych marek, generując przychody na poziomie kilkudziesięciu do kilkuset milionów złotych rocznie.

A przecież w gąszczu polskich firm ochroniarskich jest jeszcze sporo małych i średnich podmiotów. Jak w tym wszystkim się połapać i którą agencję wybrać? Po pierwsze, to co powinno być dla Ciebie najważniejsze, to koncesja. Od każdej agencji możesz wymagać okazania stosownego dokumentu potwierdzającej jej możliwości.

Koncesję wydaje Ministerstwo Spraw Wewnętrznych i Administracji. Upoważnia ona agencje do ochrony osób i mienia. Każda dobra firma ochroniarska będzie mieć taką koncesję i często można znaleźć je na ich stronach.

Jak wskazuje Dziennik Internautów – inną ważną kwestią pozostaje wykupiona polisa OC. **Od każdej firmy ochroniarskiej masz prawo domagać się okazania ubezpieczenia**. Dziennik Internautów podkreśla też, że aby zweryfikować agencję, warto poprosić ją o deklarację dotyczącą form zatrudnienia pracowników, a nawet zaświadczenia o niezaleganiu z podatkami.

Dlaczego jest to ważne? Ochroniarze zatrudniani na tzw. umowy śmieciowe, za niską stawkę, raczej niechętnie będą bronić Twojego mienia czy osoby, jeśli naraziłoby to ich zdrowie czy życie. Nie mówiąc już o pracownikach zatrudnianych „na czarno”.

Biuro ochrony możesz też poprosić o listę obiektów, które pozostają pod jej opieką – to pozwoli Ci zweryfikować, z kim dana agencja współpracuje. Możesz nawet odwiedzić, którąś z tych nieruchomości i zobaczyć, jak prezentują się poszczególni pracownicy oraz jak miejsce jest zabezpieczone technicznie. Dzięki temu sprawdzisz, czy nie ma tam np. ochroniarzy w kiepskiej kondycji fizycznej, którzy działają na zasadzie: „przynajmniej ktoś się kręci wokół". Pamiętaj, że dobra firma ochroniarska jest transparentna i niczego nie będzie ukrywać.

AGENCJA OCHRONY – DUŻA CZY MAŁA?

Przy wyborze biura ochrony rodzi się też pytanie, czy postawić na podmiot duży, czy mały. Cóż, sprawa na papierze jest dość prosta – wszystko zależy od tego, jakim budżetem dysponujesz. Jeśli nie masz zbyt wielu pieniędzy albo nie musisz ochraniać wielu ruchomości i nieruchomości, lepiej wybrać mniejszą organizację. Agencje z sektora MMŚP mają często atrakcyjniejsze stawki dla swoich klientów.

Nie daj się jednak zwieźć. Jeśli kilkudziesięcioosobowa lokalna firma ochroniarska oferuje ochro-

nę stacjonarną, patrole interwencyjne, zabezpieczanie wydarzeń, konwojowanie gotówki, a do tego usługi detektywistyczne, żadna z tych usług nie będzie wykonana dobrze. Z bardzo prostej przyczyny – taka agencja nie dysponuje wystarczającymi środkami i zasobami ludzkimi, żeby zabezpieczać wiele obiektów i klientów naraz.

Jeśli nie masz dużego budżetu – zdecyduj się na agencję wyspecjalizowaną w konkretnych obszarach, np. konwojowaniu gotówki. A jeżeli masz więcej pieniędzy i obiektów do ochrony – możesz śmiało wybierać w dużych agencjach czy wręcz korporacjach.

CO DOBRA AGENCJA POWINNA CI ZAPEWNIĆ?

Załóżmy, że zależy Ci stricte na ochronie mienia. Porządna firma ochroniarska powinna nie tylko oddelegować pracowników do zabezpieczania obiektu, ale też zainstalować i obsługiwać monitoring – łącznie z systemem alarmowym. Takie zabezpieczenie techniczne jest o tyle ważne, że zwiększa prawdopodobieństwo wykrycia kradzieży, aktu wandalizmu itd., ale też ułatwia pracę samej ochrony i weryfikuje ją.

Jeśli pracownicy ochrony znajdują się w obiekcie fizycznie, a nie tylko doraźnie w ramach patroli interwencyjnych – dobra agencja powinna też oddelegowywać inspektora, który będzie sprawdzać, jak funkcjonują ochroniarze. Zakres i częstotliwość tzw. kontroli patroli inspektorskich możesz określić z firmą w umowie.

Agencja powinna też oddelegować jakiegoś pracownika, który będzie z Tobą w stałym kontakcie. Dzięki temu firma będzie od razu reagować na zgłaszane przez Ciebie uwagi czy sugestie. Jeśli agencja nie oddelegowuje konkretnej, dyspozycyjnej osoby, a Ty nie wiesz do kogo masz zadzwonić – to powinna być dla Ciebie czerwona lampka. Nie ma sensu działać z taką organizacją. W końcu w przypadku bezpieczeństwa liczy się szybkość. A gdzie tu mowa o szybkości działania, kiedy Twoja prośba przechodzi przez kilka osób czy departamentów?

Reasumując – od agencji masz prawo wymagać okazania koncesji, potwierdzenia wykupienia polisy OC, deklaracji dot. formy zatrudnienia czy zaświadczenia o niezaleganiu z podatkami.

Czego możesz wymagać od firmy ochroniarskiej?

W kompetencji dobrej firmy ochroniarskiej pozostaje instalacja i obsługa monitoringu, kontrola patroli inspektorskich czy oddelegowanie dyspozycyjnego pracownika do kontaktu z Tobą. Pamiętaj, że na bezpieczeństwie nie warto oszczędzać. Nie decyduj się na agencję, która nie ma ważnych koncesji, płaci pracownikom pod stołem czy oszczędza na ich i Twoim bezpieczeństwie.

W TWOJEJ FIRMIE
ZDARZYŁ SIĘ

WYCIEK DANYCH OSOBOWYCH?

MOŻEMY CI POMÓC

SPRAWDŹ JAK

Polityka® Bezpieczeństwa

SECURITYMAGAZINE.PL

BEZPIECZEŃSTWO PRZECHOWYWANIA DANYCH W SYSTEMIE CRM ORAZ ERP W CHMURZE

Daria Sadowska
Firmao

Przyspieszenie tempa cyfryzacji przedsiębiorstw przybrało na sile w ostatnim roku, głównie za sprawą pandemii, która dotknęła cały świat. Jednym z ważniejszych elementów cyfryzacji jest wykorzystanie rozwiązań chmurowych w biznesie.

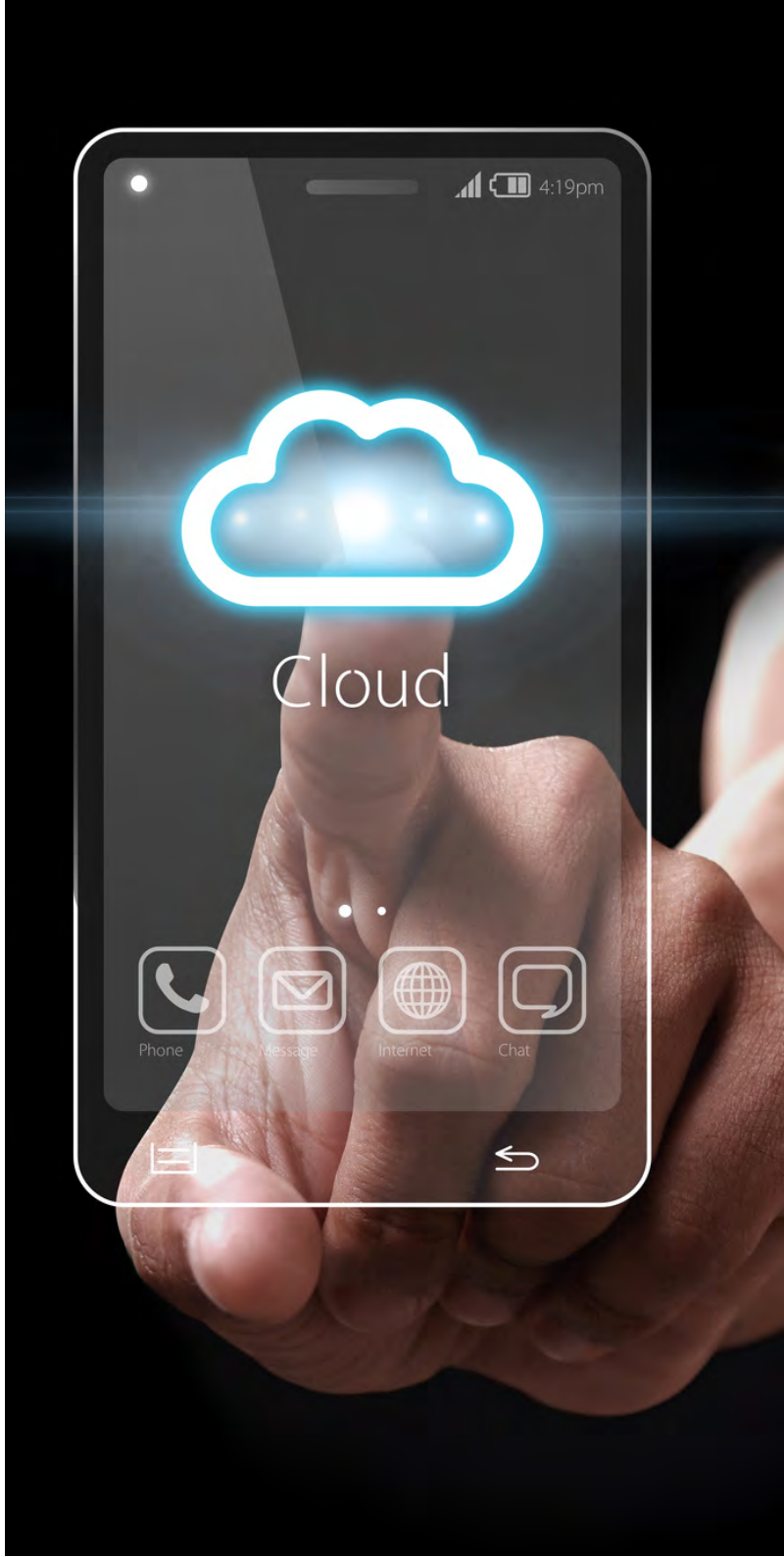
CHMURA OBLICZENIOWA

Chmura obliczeniowa (ang. cloud computing) to model korzystania z usług IT, który charakteryzuje się umieszczeniem wszystkich lub części zasobów firmy na zewnętrznym serwerze, który nie jest bezpośrednio zarządzany przez organizację. Usługa jest dostarczana za pośrednictwem Internetu i jest dostępna z dowolnego miejsca, o dowolnej porze.

Badania wskazują, że coraz więcej firm będzie decydowało się na implementację usług chmurowych w ciągu kolejnych 10 lat. Według Global Market Insights do 2026 roku 75% przedsiębiorstw w UE będzie korzystać z chmury, sztucznej inteligencji czy big data.

Sytuacja wygląda optymistycznie także w Polsce, ponieważ według opublikowanego w marcu 2021 badania EY Polska „Transformacja cyfrowa firm 2020" aż 64% polskich przedsiębiorstw wdrożyło rozwiązania chmurowe, a na przestrzeni najbliższych 12-18 miesięcy zdecyduje się na to 26% ankietowanych.

Z tego badania wynika jeszcze jedna ważna informacja. Wskazuje się, że jako jedną z największych barier we wdrażaniu usług chmurowych w polskich przedsiębiorstwach pozostaje brak zaufania, który deklaruje 29% firm. Przedsiębiorstwa mają wątpliwości w zakresie bezpieczeństwa chmury.



NA RYSUNKU PRZEDSTAWIONO NAJWAŻNIEJSZE MOTYWY PRZENIESIENIA ZASOBÓW FIRMY DO CHMURY.

Temat bezpieczeństwa danych w chmurze budzi największą obawę wśród przedsiębiorców sektora MSP. W końcu w systemach CRM (system informatyczny, który automatyzuje i wspomaga procesy na styku klient-organizacja w zakresie pozyskania oraz utrzymania klienta, czyli system wspomagający pracę działów: marketingu, sprzedaży, obsługi klienta, zarządu) oraz ERP (system do efektywnego planowania oraz zarządzania całością za-

sobów przedsiębiorstwa) właściciele firm chcą przechowywać wszystkie dane dotyczące firmy np. ilość pracowników, dane klientów, faktury, stany magazynowe. Tego typu informacje są jedną z najważniejszych informacji przedsiębiorstwa. Na szczęście backupowanie oraz przechowywanie danych online, a nie w siedzibie firmy może okazać się o wiele bezpieczniejsze. Kopie zapasowe danych są zabezpieczane na serwerach dostawcy backupu w innej lokalizacji niż firma, dzięki czemu nawet fizyczne zniszczenie sprzętu przedsiębiorstwa w wyniku np. kataklizmów naturalnych, nie doprowadzi do ich utraty. Skłonność do wyboru rozwiązania online z pewnością rośnie, kiedy jego dostawcy są w stanie udowodnić firmom, że bezpieczeństwo danych w chmurze spełnia najwyższy poziom.

ZALETY PRZECHOWYWANIA DANYCH W CHMURZE

Technologie chmurowe są integralną częścią świata biznesu. Przedsiębiorstwa chętnie sięgają po takie rozwiązania z kilku powodów.
Po pierwsze - o wiele wygodniej jest korzystać z popularnych platform, niż tworzyć własny system komunikacji i zarządzania projektem. Dzięki pracy w chmurze każdy pracownik posiada stały dostęp do danych oraz dokumentów i może mieć wgląd w zawartość z każdego miejsca na świecie, do którego oczywiście dociera Internet. Jest to znaczące ułatwienie pracy, zwłaszcza w firmach nastawionych na pracę w systemie projektowym. Drugą kwestią są finanse. Rozwiązania zewnętrzne są znacznie tańsze. Zakup własnych systemów, czy serwerów wymaga wysokich nakła-

dów finansowych, a w przypadku działania w chmurze, można bez przeszkód korzystać z infrastruktury udostępnianej przez dostawcę.

Do głównych korzyści wynikających z korzystania z usług chmurowych należą:

- oszczędność pieniędzy,
- awarie sprzętu nie skutkują utratą danych,
- elastyczność/możliwość pracy zdalnej z każdego miejsca na świecie,
- ułatwienie współpracy organizacyjnej,
- ochrona danych.

PRACA NA SERWERACH OD FIRMY AMAZON

Jedną z licznych zalet wielu systemów CRM i ERP jest to, że działają one w chmurze – Amazon Web Services. Dzięki temu każdy użytkownik może korzystać z systemów poza biurem. Jest to niezwykle przydatne szczególnie dla dyrektorów na konferencjach czy delegacjach oraz pracowników pracujących w terenie.

Używanie programu w chmurze pozwala także uniezależnić się od jednego, konkretnego sprzętu – z najpopularniejszego polskiego oprogramowania CRM i ERP Firmao można korzystać z dowolnego komputera, a także z urządzeń mobilnych.

Korzystanie z oprogramowania w chmurze jest bardzo wygodne, jednak niektórzy zastanawiają się także, czy dane w chmurze są tak samo bezpieczne, jak w oprogramowaniach stacjonarnych, które są instalowane na osobnych komputerach.

SERWERY NAJPOPULARNIEJSZEGO POLSKIEGO OPROGRAMOWANIA

Firmao pracuje na serwerach EC2, za których jakość odpowiada firma Amazon. Serwery firmy Amazon znajdują się w Irlandii oraz w Niemczech. Dokładne miejsca, gdzie znajdują się serwerownie są objęte ścisłą tajemnicą, przeznaczoną dla nielicznych. Na Mapach Google nie znajdziemy budynków z wielkim logiem firmy Amazon na dachu. Serwery znajdują się w pilnie strzeżonych niepozornych budynkach. Nawet pracownicy firmy Amazon mają ograniczony wgląd do serwerów – mogą do nich wejść, jeśli tylko mają poważny powód pozwalający na dostęp. Jednak po uzyskaniu pozwolenia muszą potwierdzić swoją tożsamość w licznych, skomplikowanych zabezpieczeniach. Dlatego uważa się, że serwerownie, z których korzysta Firmao to jedne z najlepiej strzeżonych miejsc na świecie.

BEZPIECZEŃSTWO DANYCH OSOBOWYCH W CHMURZE

AWS angażuje niezależnych audytorów zewnętrznych, aby spełniać odpowiednie wymogi bezpieczeństwa. Kontrole te są przeprowadzane nie rzadziej niż co 6 miesięcy i zachowują standardy audytu AICPA i ISO27001 lub innych równoważnych.

Amazon posiada także jeden z najważniejszych certyfikatów bezpieczeństwa ISO 27001 oraz spełnia normę bezpieczeństwa Level 1 w kategorii Data Security Standards (DDS).

AWS deklaruje zgodność z przepisami Dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 roku w sprawie ochrony osób fizycznych w zakre-sie przetwarzania danych osobowych oraz swobodnego przepływu tych danych, która stanowi wykładnię w kwestii przechowywania danych osobowych.

PODSUMOWANIE

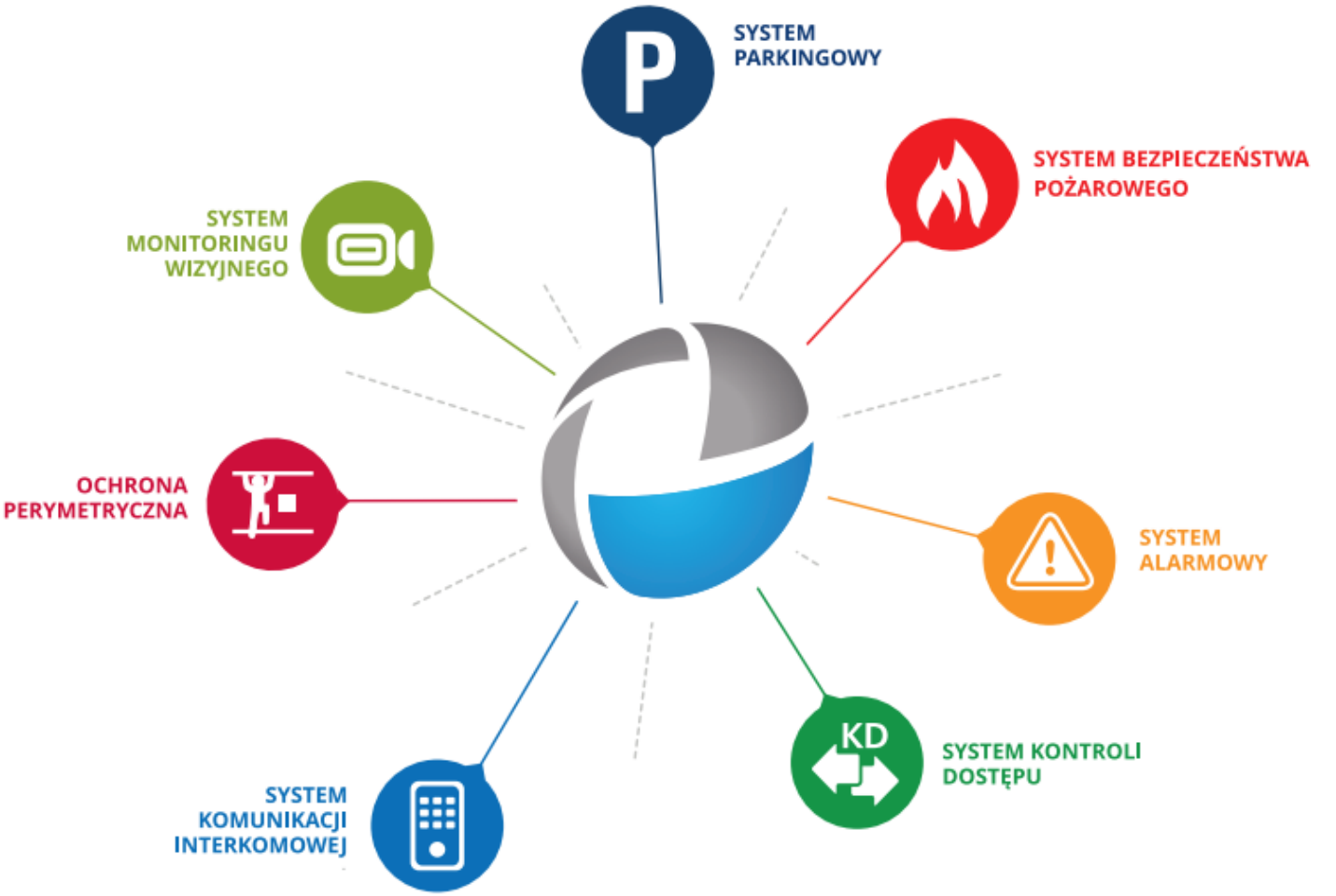
Chmura to przyszłość, za kilka lat będzie to już naturalny wybór. Aktualnie liczba argumentów przemawiających za wyborem systemu CRM oraz ERP w chmurze jest na tyle duża, że potrzeba naprawdę ogromnej niechęci bądź uwarunkowań prawnych, aby „z miejsca" odrzucić ten model wdrożenia. Takie rozwiązanie zdecydowanie pomoże w optymalizacji procesów biznesowych w przedsiębiorstwie. Jest bezpieczne, zapewnia dostęp do danych 24/7/365 dni w roku z dowolnego urządzenia na świecie połączonego z Internetem, jak również może stanowić pierwszy krok ku oszczędnościom i redukcji posiadanego „długu technologicznego".

Oprogramowanie
klasy PSIM+

System zarządzania informacją o bezpieczeństwie fizycznym

C & C solution partner

winguard always retain control



www.ccpartners.pl

ZARZĄDZANIE BEZPIECZEŃSTWEM W URZĘDACH

Tobiasz Bąkowski
C&C Partners

Budynki administracji państwowej muszą spełniać szereg wymogów, aby podnieść komfort i efektywność pracy urzędników oraz zapewnić bezpieczeństwo zarówno osób, jak i budynków. Ponadto w tym segmencie rynku często pojawia się konieczność redukcji kosztów utrzymania oraz zwiększenia efektywności pracy personelu.

BEZPIECZEŃSTWO DOSTOSOWANE DO POTRZEB

Różnorodne obiekty administracji państwowej wymagają elastycznego dopasowania rozwiązań do indywidualnych potrzeb klienta oraz obowiązujących przepisów. Systemy zabezpieczeń mogą zostać wdrożone jako pojedyncze rozwiązania lub jako zintegrowany system zarządzania bezpieczeństwem i komunikacją, gwarantujący modularną rozbudowę oraz otwarte interfejsy dla innych urządzeń działających na terenie obiektów. Takie podejście gwarantuje bezpieczeństwo inwestycji oraz możliwość jej rozbudowy w czasie.

Szeroka gama technologicznych rozwiązań pozwala sprostać takim wyzwaniom, jak:

- kontrola osób przebywających i odwiedzających obiekt
- zarządzanie dostępem do określonych części budynku
- obsługa gości
- monitorowanie określonych obszarów
- zarządzanie parkingiem dla pracowników oraz petentów.

KONTROLOWANY DOSTĘP DO POMIESZCZEŃ

Bezpieczeństwo w budynkach administracji państwowej to w znaczącej mierze kontrola osób wpuszczanych do obiektu lub wydzielonych jego części. Po pierwsze system kontroli dostępu zabezpiecza przed nieautoryzowanym dostępem do ciągów komunikacyjnych i kluczowych pomieszczeń m.in. archiwum, serwerowni oraz pomieszczeń technicznych. Po drugie rozwiązanie to pozwala na zarządzanie dostępem do poszczególnych pięter budynku już na poziomie wind. Wdrożenie integracji systemu kontroli dostępu z systemem zarządzania windami skutkuje tym, że system kontroli dostępu przekazuje informacje o uprawnieniach użytkownika do

systemu zarządzania windami. Zwrotnie użytkownik otrzymuje na wyświetlaczu informację, do której windy powinien się kierować.

Kolejnymi zaletami tego systemu są funkcje zwiększające jego niezawodność m.in. anty-passback przy bramkach w części wejściowej do budynku oraz zmiana trybu działania czytników, bramek uchylnych i tripodów z poziomu intuicyjnego interfejsu. **Uzupełnieniem systemu kontroli dostępu jest opcja kompleksowej obsługi gości poprzez funkcję wcześniejszego przygotowania kart dostępowych dla interesantów, ważnych gości lub stażystów. Dodatkowo rozwiązanie to umożliwia wcześniejszą rezerwację odpowiedniej ilości miejsc parkingowych dla gości.**

Pełne monitorowanie osób przemieszczających się w ramach obiektu umożliwia usprawnienie ewentualnych działań ewakuacyjnych i weryfikację obecności osób w poszczególnych lokalizacjach (np. w dniu dokonania kradzieży).

WYKRYWANIE I WERYFIKACJA ZDARZEŃ ALARMOWYCH

Przy dużych obiektach urzędowych, kluczowe jest zautomatyzowanie procesów detekcji i weryfikacji działań alarmowych.
Systemem, który stricte odpowiada za bezpieczeństwo danego obiektu jest system sygnalizacji włamania i napadu. Umożliwia on sygnalizację nieautoryzowanego wejścia do danego budynku administracji państwowej.

Natomiast, aby zwiększyć jego efektywność, przyciski napadowe są instalowane na stanowiskach recepcji, a pracownicy ochrony są wyposażani w bezprzewodowe przyciski sygnalizujące napad. Dodatkowo pomieszczenia są zabezpieczane detektorami ruchu, a ich pełna wizualizacja wraz z ich statusami oraz przypisanymi strefami jest dostępna na stanowisku ochrony.

Operator otrzymuje klarowną informację o typie alarmu oraz lokalizacji źródła alarmu na mapie synoptycznej wraz z podglądem ze skorelowanej kamery IP analizującej obraz. Dodatkowo prezentowana jest jasna instrukcja postępowania w postaci interaktywnych kroków zależnych od typu i lokalizacji alarmu.

INTELIGENTNA ANALIZA OBRAZU Z KAMER

Nieodzownym systemem budynkowym poprawiającym bezpieczeństwo i jakość pracy w placówkach administracji państwowej jest inteligentny system monitoringu wizyjnego obiektu z analizą obrazu. W ramach systemu realizowany jest monitoring wizyjny terenu zewnętrznego u-

rzędu (parkingi, wejścia do budynku), a także monitoring wnętrza obiektu zapewniający podgląd ciągów komunikacyjnych i kluczowych pomieszczeń w budynkach. Natomiast wypracowane zaawansowane rozwiązania bazujące na sztucznej inteligencji umożliwiają obserwację obrazu wysokiej jakości „na żywo" przez pracowników ochrony oraz wykorzystanie algorytmów analizy obrazu m.in. rozpoznawanie twarzy, czy tablic rejestracyjnych.

SPRAWNA KOMUNIKACJA

System komunikacji interkomowej dla obiektów administracji państwowej pozwala na komunikację osób za pomocą interkomów w architekturze punkt-punkt i punkt-wiele punktów, nadawanie komunikatów zbiorowych z podziałem na poszczególne części budynku oraz zainstalowanie stacji nabiurkowych w pomieszczeniach sekretariatu, ochrony oraz recepcji. Ważnym elementem tego systemu jest integracja z monitoringiem wizyjnym, dzięki czemu jest możliwe nagrywanie wybranych rozmów interkomowych w korelacji z obrazem z kamery CCTV.

ZARZĄDZANIE PARKINGIEM

Rozwiązanie z obszaru zarządzania parkingiem pozwala na kontrolowanie dostępu do parkingu urzędu dla pracowników i petentów oraz zapewnienie odpowiedniej liczby miejsc osobom niepełnosprawnym. Kontrola dostępu na terenie parkingu jest realizowana w oparciu o czytniki dalekiego zasięgu lub analizę tablic rejestracyjnych. Natomiast komunikacja z ochroną i służbą parkingową odbywa się za pomocą systemu interkomowego.

INTEGRACJA Z SYSTEMAMI TRZECIMI

W ramach integracji z systemami dostawców trzecich, inteligentne systemy umożliwiają integrację z systemami sterowania windami, systemami sygnalizacji pożarowej, systemami

zarządzania kluczami. Dzięki temu w znaczący sposób można rozbudować funkcjonalności rozwiązań budynkowych w celu bardziej efektywnego zarządzania budynkami. Szerokie możliwości integracyjne pozwalają, aby w sposób efektywny rejestrować czas pracy. System rejestracji czasu pracy urzędników i pozostałych pracowników administracyjnych umożliwia wsparcie dla specjalnych aktywności np. wyjście prywatne, do lekarza itp. Rozwiązanie posiada zaawansowany system generowania raportów oraz opcję integracji z systemami kadro-płacowymi wykorzystywanymi przez urząd.

ZARZĄDZANIE Z POZIOMU JEDNEGO PULPITU

Efektywne zarządzanie bezpieczeństwem to przede wszystkim zebranie informacji ze wszystkich zdarzeń w jednym miejscu. Do tego służy rozwiązanie przeznaczone do monitoringu i zarządzania wszystkim systemami z jednego stanowiska operatorskiego w ramach jednego centrum nadzoru.

Oprogramowanie PSIM+ umożliwia efektywne monitorowanie i zarządzanie procesami bezpieczeństwa. Integruje różnorodne podsystemy, m.in. kontroli dostępu, sygnalizacji włamania czy

napadu, monitoringu wizyjnego, interkomowy, parkingowy, rejestracji czasu pracy, czy sygnalizacji pożarowej. Dzięki rozbudowanym interfejsom, możliwa jest integracja dowolnego innego systemu wymaganego przez inwestora.

Rozbudowane narzędzia raportujące zdarzenia w oprogramowaniu PSIM+ pozwalają na odpowiednie raportowanie zdarzeń oraz istotnych informacji o zasobach i funkcjonowaniu poszczególnych systemów.

Odpowiednie zarządzanie zgromadzoną wiedzą przekłada się na możliwość optymalnego zarządzania wieloma obiektami oraz porządkowanie obowiązujących w określonym obiekcie procedur, co przekłada się na optymalizację kosztów.

OBSŁUGA PRAWNA E-COMMERCE

WWW.RZETELNYREGULAMIN.PL

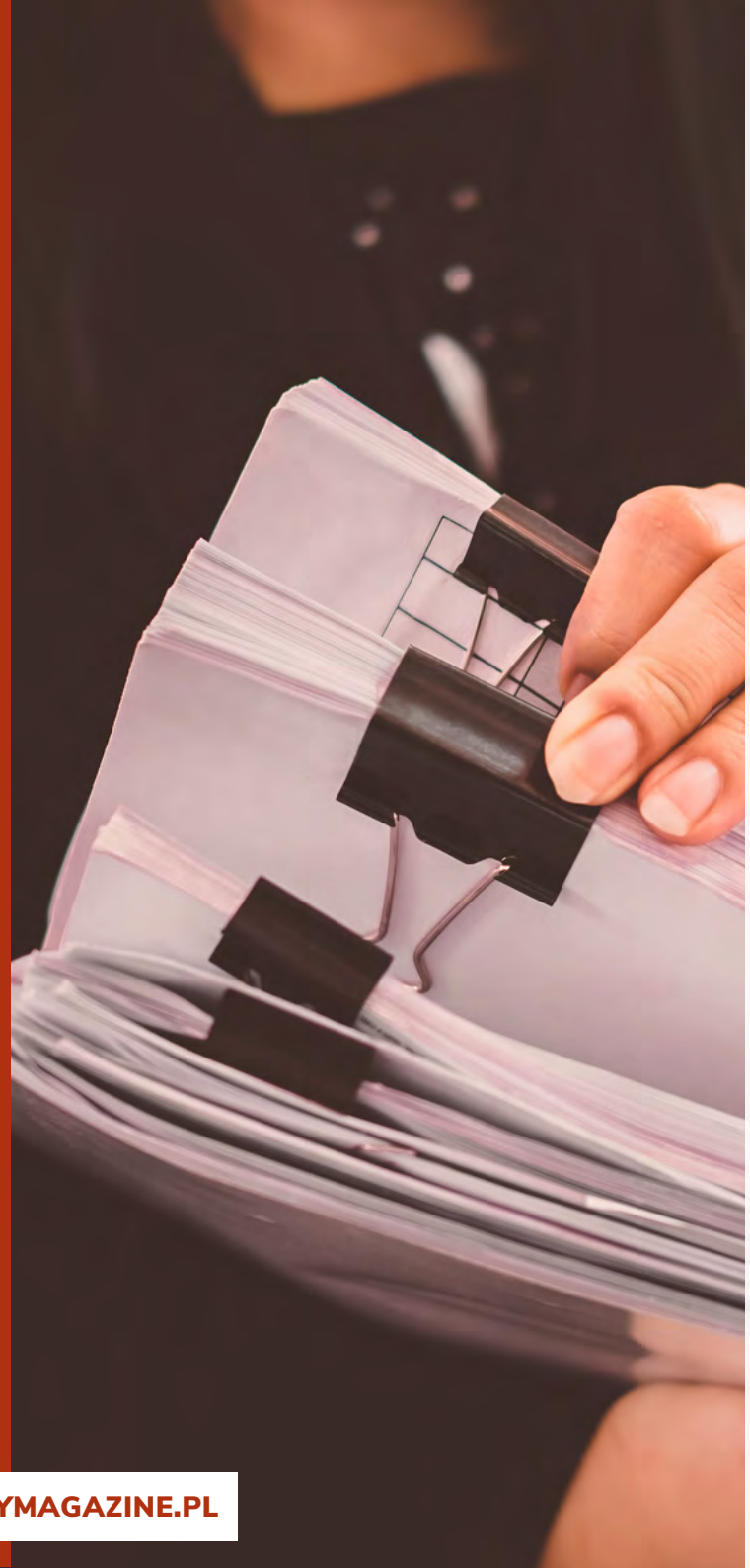
SECURITYMAGAZINE.PL

OSZUSTWA "NA PREZESA" ORAZ "NA FUNDUSZE EUROPEJSKIE"

insp. dr Mariusz Ciarka
Komenda Główna Policji

POLICJA

W działaniach oszustów pojawiają się ciągle nowe sposoby, a wszystko po to aby łatwo i szybko wzbogacić się. Oszuści często oferują swoją „pomoc" w załatwieniu różnych spraw bez zbędnych formalności w urzędach. Niestety, po jakimś czasie okazuje się, że zostaliśmy celowo wprowadzeni w błąd, a przekazane wcześniej pieniądze przepadły.



"NA FUNDUSZE EUROPEJSKIE"

Ofiarami oszustów padają nie tylko osoby prywatne, ale także ci którzy posiadają własne firmy i prowadzą działalność gospodarczą. Oszuści swoją przestępczą działalność kierują na placówki administracji publicznej, składając swoją ofertę rzekomej pomocy. Nie wszyscy jednak, których oszukano, zgłaszają ten fakt organom ścigania, zwłaszcza, jeśli stracili niewielką ilość pieniędzy.

Powszechnie wiadomo, że od momentu wejścia Polski do Unii Europejskiej, osoby prywatne, jak i instytucje mogą starać się o pozyskanie funduszy na rozwój firmy lub też na rozpoczęcie działalności gospodarczej. Niestety, **ten fakt wykorzystują oszuści**. Ogłaszając się w internecie lub kontaktując się bezpośrednio z zainteresowanym telefonicznie, **oferują do zakupu komplet wypełnionych już dokumentów**, które wystarczy tylko złożyć w odpowiedniej placówce, co będzie następnie skutkowało przyznaniem dotacji z unijnych funduszy. Dodatkową zachętą jest dołączenie wzoru albo wręcz gotowego biznesplanu oraz **powoływanie się na współpracę z ministerstwem pracy lub Eurocentrami**. Za taki komplet dokumentów trzeba zapłacić od 150 do ponad 200 złotych. Niestety, prawda okazuje się bolesna, gdyż wpłacone pieniądze przepadły, a otrzymane dokumenty nie skutkują automatycznym przyznaniem dotacji.

Należy podkreślić, że dokumenty, które oszuści przysyłają, są ogólnie dostępne w internecie, urzędach oraz Eurocentrach, zajmujących się środkami unijnymi. Są to dokumenty bezpłatne, często też pobierane przez oszustów bezpośrednio w tych punktach.

JAK NIE DAĆ SIĘ OSZUKAĆ?

Starając się o uzyskanie unijnej dotacji, najlepiej osobiście zasięgnąć w tym zakresie informacji w punktach obsługi klienta, znajdujących się w Eurocentrach czy też urzędach pracy. Tam na pewno otrzymamy rzetelną i fachową informację o procedurach związanych z uzyskaniem dotacji.

PAMIĘTAJMY, ABY TAKICH SPRAW NIGDY NIE ZAŁATWIAĆ TELEFONICZNIE I PRZEDE WSZYSTKIM NIE WPŁACAĆ ŻADNYCH PIENIĘDZY, KTÓRE CZĘSTO SĄ NIE DO ODZYSKANIA.

NA PREZESA

Uwaga na oszustów podających się za prezesów firm. Wysyłają oni do pracowników wiadomości z poleceniem wykonania pilnego przelewu. Pieniądze trafiają jednak na zagraniczne konta oszustów. **Mowa tu o metodzie na tak zwanego prezesa.**

Oszuści posługują się znajomością struktury firmy oraz danymi personalnymi pracowników. Wykorzystują fakt, że w większych firmach znaczna część komunikacji między działami odbywa się drogą elektroniczną. **Policjanci na terenie całego kraju przestrzegają, że adres e-mailowy którym posługują się przestępcy, może być łudząco podobny do firmowego.** Często też polecenie wykonania przelewu wysyłane jest dopiero w kolejnych wiadomościach – wcześniej prowadzona korespondencja ma uśpić czujność pracownika. Finalnie okazuje się, że prawdziwy prezes żadnych przelewów nie zlecał, a pieniądze trafiły na konta oszustów. Wiadomości natomiast wysyłane były za pośrednictwem zagranicznych serwerów. **Aby ustrzec się przed oszustami najlepiej osobiście potwierdzić polecenie wykonania przelewu. Należy również baczniej przyjrzeć się adresom, z których wysyłane są wiadomości.**

impero 360
by UNICARD

UNICARD

More than access control!

Poznaj impero 360 - skalowalną Platformę w chmurze

do Zarządzania Ruchem Osób!

www.impero360.cloud

SECURITYMAGAZINE.PL

SYSTEM KONTROLI DOSTĘPU DRZWI. JAK WYBRAĆ?

Maciej Misaczek
UNICARD SA

Czym jest kontrola dostępu i jak działa? Gdzie znajduje zastosowanie i na co zwrócić uwagę podczas wyboru systemu kontroli dostępu? Na te i inne pytania, odpowiadamy w poniższym artykule.

CZYM JEST KONTROLA DOSTĘPU?

Kontrola dostępu to zespół środków fizycznych i programowych, dzięki którym można zarządzać dostępem poszczególnych osób do pomieszczeń, stref, budynków, a nawet sieci budynków rozmieszczonych na większym obszarze. System kontroli dostępu znajduje zastosowanie także w zarządzaniu wjazdem pojazdów na określony teren.

Takie rozwiązanie można wykorzystać m.in. w biurowcach. Jeżeli w budynku pracuje kilka niezależnych od siebie firm, zarządca obiektu może wprowadzić system kontroli dostępu, dzięki któremu każda osoba pracująca w biurze będzie miała z góry określony dostęp do wybranych miejsc w konkretnym przedziale czasowym.

Zarządzanie dostępem jest zautomatyzowane i przyczynia się do poprawy bezpieczeństwa wszystkich, którzy korzystają z budynku.

W JAKI SPOSÓB DZIAŁA KONTROLA DOSTĘPU DO DRZWI?

W skład systemu kontroli dostępu wchodzą urządzenia oraz oprogramowanie. Urządzenia to m.in. czytniki, które instaluje się w pobliżu wejść czy karty zbliżeniowe, rozwiązania na telefon (z technologią NFC bądź Bluetooth). Można wykorzystać także weryfikację biometryczną – np. dzięki odciskowi palca lub przez skan tęczówki.

Zadaniem czytnika jest pobranie danych z identyfikatora i przesłanie ich do sterownika. To on odczytuje informacje o tym, czy dany użytkownik posiada dostęp do danego obiektu. W przypadku, gdy system rozpozna i zweryfikuje użytkownika, rygle elektromagnetyczne zwolnią się, a drzwi się otworzą.

ZALETY SYSTEMU KONTROLI DOSTĘPU

Dlaczego systemy kontroli dostępu wypierają klucze? To nowoczesne rozwiązanie, które przeważa wygodą i **znacznie zwiększa bezpieczeństwo**. Dodatkowo, identyfikatory nie wymagają kontaktu fizycznego, dzięki czemu korzystanie z takiego rozwiązania jest po prostu szybsze. To szczególnie ważne w przypadku szlabanów parkingowych czy w magazynach lub halach produkcyjnych.

Co więcej – aby przejścia były odpowiednio zabezpieczone, każdy zamek potrzebuje osobnego klucza. W przypadku kontroli dostępu, jedna karta wystarczy, by otworzyć wszystkie przejścia, co jest bardzo praktycznym rozwiązaniem w budynkach, które posiadają wiele przejść.

Sporą przewagą jest możliwość zdalnego zarządzania dostępem dla uprawionych osób. Pracownicy, którzy odchodzą z firmy lub otrzymują dostęp do innych pomieszczeń, nie muszą pojawiać się fizycznie, aby odebrać lub oddać klucze. Zarządzanie uprawieniami odbywa się na poziomie administratora oprogramowania, który zdalnie odbiera lub nadaje dostęp.

Może też zablokować dostęp, jeżeli karta została zgubiona lub skradziona.

System umożliwia także monitorowanie ruchu w obiekcie – administrator otrzymuje dostęp do informacji o tym, kto i kiedy wyszedł z budynku lub pomieszczenia. To nie tylko poprawa sprawności zarządzania personelem, ale również przydatna funkcja np. podczas nadużyć lub ewakuacji.

System kontroli dostępu jest **skalowalny**. Obsługuje nie tylko drzwi, ale także szlabany parkingowe. Co istotne, kontrolę dostępu można zintegrować z innym oprogramowaniem – chociażby z systemem rejestracji czasu pracy. Kontakt identyfikatora z czytnikiem otworzy drzwi i zarejestruje początek i koniec pracy.

System rozwija się wraz z firmą. Uprawienia dla nowych pracowników lub do nowych miejsc można nadać w każdej chwili. Urządzenia KD mogą działać na podstawie wspólnej bazy danych i być zainstalowane w różnych lokalizacjach.

ZASTOSOWANIE SYSTEMÓW DOSTĘPU

Chociaż rozwiązania kontroli dostępu kojarzą się przede wszystkim z biurowcami i halami produkcyjnymi, tak naprawdę zdadzą egzamin na każdym terenie, który potrzebuje monitoringu ruchu oraz wydzielenia stref dla konkretnych użytkowników. System KD znajdzie zastosowanie między innymi w:

- **budynkach mieszkalnych** – każdy mieszkaniec otrzyma indywidualny identyfikator, dzięki któremu zyska dostęp do osiedlowego parkingu, wejścia do budynku, piwnicy czy mieszkania;
- **hotele i pensjonaty** – pracownicy zyskują dostęp do określonych stref w tego typu obiektach, w związku z czym zwiększa się poziom bezpieczeństwa gości oraz ich mienia;
- **banki** – placówki bankowe zobowiązane są do przestrzegania przepisów związanych z przechowywaniem danych wrażliwych oraz ograniczenia dostępu do miejsc, w których znajduje się dokumentacja. Stąd konieczność nadania różnych uprawnień z zakresu kontroli dostępu różnym pracownikom;
- **biura** – system kontroli dostępu nie tylko pozwala nadawać i kontrolować dostęp pracownikom, ale chroni dokumentację czy sprzęt;
- **szpitale, przychodnie** – podobnie jak banki, placówki medyczne i obiekty służby zdrowia zobowiązane są do przechowywania i ochrony danych osobowych pacjentów oraz informacji o ich zdrowiu. Także sprzęt, leki i wszelkie wyroby medyczne muszą być chronione m.in. przed kradzieżą. System kontroli dostępu upoważnia zatem konkretnych pracowników do odwiedzania poszczególnych części placówek, m.in. sal operacyjnych, archiwów czy laboratoriów;
- **placówki oświatowe** – system kontroli dostępu można wykorzystać nie tylko w samych obiektach szkolnych lub uczelnianych. Jest potrzebny także w domach studenckich – dzięki wdrożeniu takiego rozwiązania, na teren akademików lub szkół z internatem nie dostanie się niepożądana osoba;
- **galerie handlowe,** obiekty sportowe, urzędy, centra konferencyjne – i wszędzie tam, gdzie najważniejsze jest bezpieczeństwo i ochrona danych.

5 RZECZY, NA KTÓRE WARTO ZWRÓCIĆ UWAGĘ, WYBIERAJĄC SYSTEM KONTROLI DOSTĘPU DRZWI

Wdrożenie systemu kontroli dostępu powinno być przemyślanym przedsięwzięciem – w końcu chroni budynek, sprzęt, dane oraz znajdujących się w nim ludzi. Przed wyborem rozwiązania, warto zadać sobie 5 zasadniczych pytań, które w końcowym etapie pomogą podjąć ostateczną decyzję.

Po pierwsze: czy system jest skalowalny?

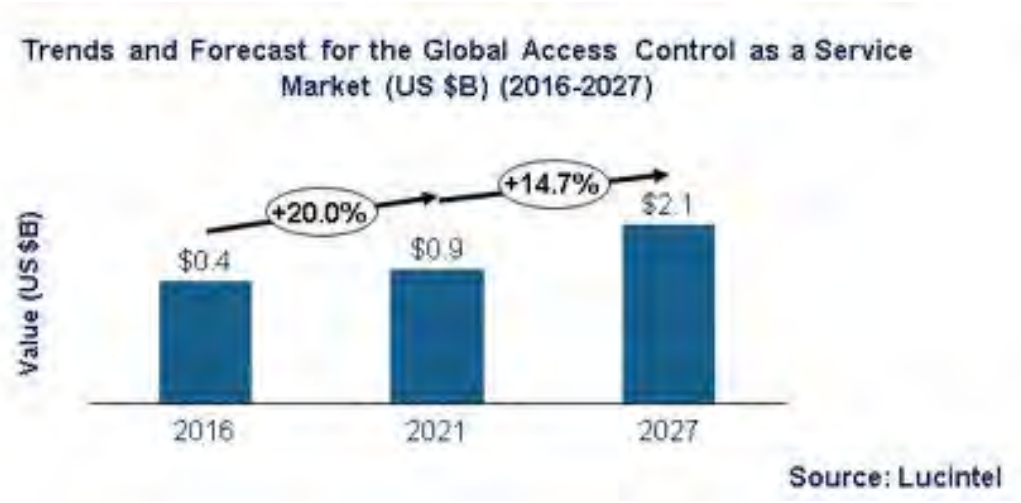
Odpowiedni system kontroli dostępu powinien rozwijać się wraz z firmą. Rozwiązanie powinno oferować możliwość dodawania kolejnych urządzeń, nowych identyfikatorów, obsługiwać kilka różnych lokalizacji.

Po drugie: czy obsługa systemu jest łatwa?

Intuicyjna obsługa systemu i czytelny, przyjazny interfejs to czynniki, które należy wziąć pod uwagę. Im prostszy będzie w obsłudze – tym lepiej. Dodawanie nowych użytkowników i zarządzanie uprawnieniami nie powinno sprawiać trudności administratorowi systemu.

Po trzecie: w jaki sposób mogę korzystać z systemu?

Oprogramowanie może być zainstalowane bezpośrednio na urządzeniu (komputerze) lub w chmurze (ACaaS – Access Control as a Service – np. impero 360). W pierwszym przypadku, administrator loguje się z konkretnego urządzenia, natomiast w drugim – z dowolnego miejsca i urządzenia, które posiada przeglądarkę www i dostęp do internetu.



SZACUNKOWY WZROST GLOBALNEGO RYNKU ACAAS DO 2027 ROKU

Po czwarte: jakie standardy bezpieczeństwa zapewnia system?

Oprócz zapewniania bezpieczeństwa w budynku, system powinien chronić także przetrzymywane w nim dane i posiadać odpowiednie zabezpieczenia, które uchronią przed niepożądanymi użytkownikami.

Po piąte: czy system może być zintegrowany z zewnętrznym oprogramowaniem?

System może współpracować z innymi aplikacjami zwiększającymi bezpieczeństwo w budynku i pomagają w zarządzaniu. Zwykle jest zintegrowany z rejestracją czasu pracy, monitoringiem wizyjnym, systemem rezerwacji sal.

System kontroli dostępu drzwi. Jak wybrać?

System kontroli dostępu to przede wszystkim większe bezpieczeństwo i bardziej intuicyjne zarządzanie dostępem w obrębie danej placówki. Dzięki możliwości integracji z innym oprogramowaniem, może zautomatyzować i usprawnić wiele procesów.

KATEGORYZACJA ALERTÓW. AI MOŻE TO ZROBIĆ ZA CIEBIE

Christian Putz
Vectra AI

Jeśli poprosimy analityków bezpieczeństwa o opisanie największych problemów, z jakimi się zmagają, otrzymamy zróżnicowane odpowiedzi. Możemy być jednak pewni, że wszyscy wskażą wyzwanie, jakim jest radzenie sobie z liczbą niemal niekończących się alertów i wynikającego z tego zmęczenia.

Z doświadczeń Vectra AI wynika, że wyzwania w tym obszarze sprowadzają się do trzech punktów:

1. W ciągu dnia nie ma wystarczająco dużo czasu, aby poradzić sobie z ilością alertów, które należy przeanalizować,
2. Bardzo trudno efektywnie wykorzystać czas, ponieważ nie można odseparować fałszywych i prawdziwych informacji o zagrożeniu,
3. Istnieją obawy, że prawdziwy atak zostanie przeoczony, ponieważ informacja o nim jest zagrzebana w szumie generowanym przez przestarzałe rozwiązanie.

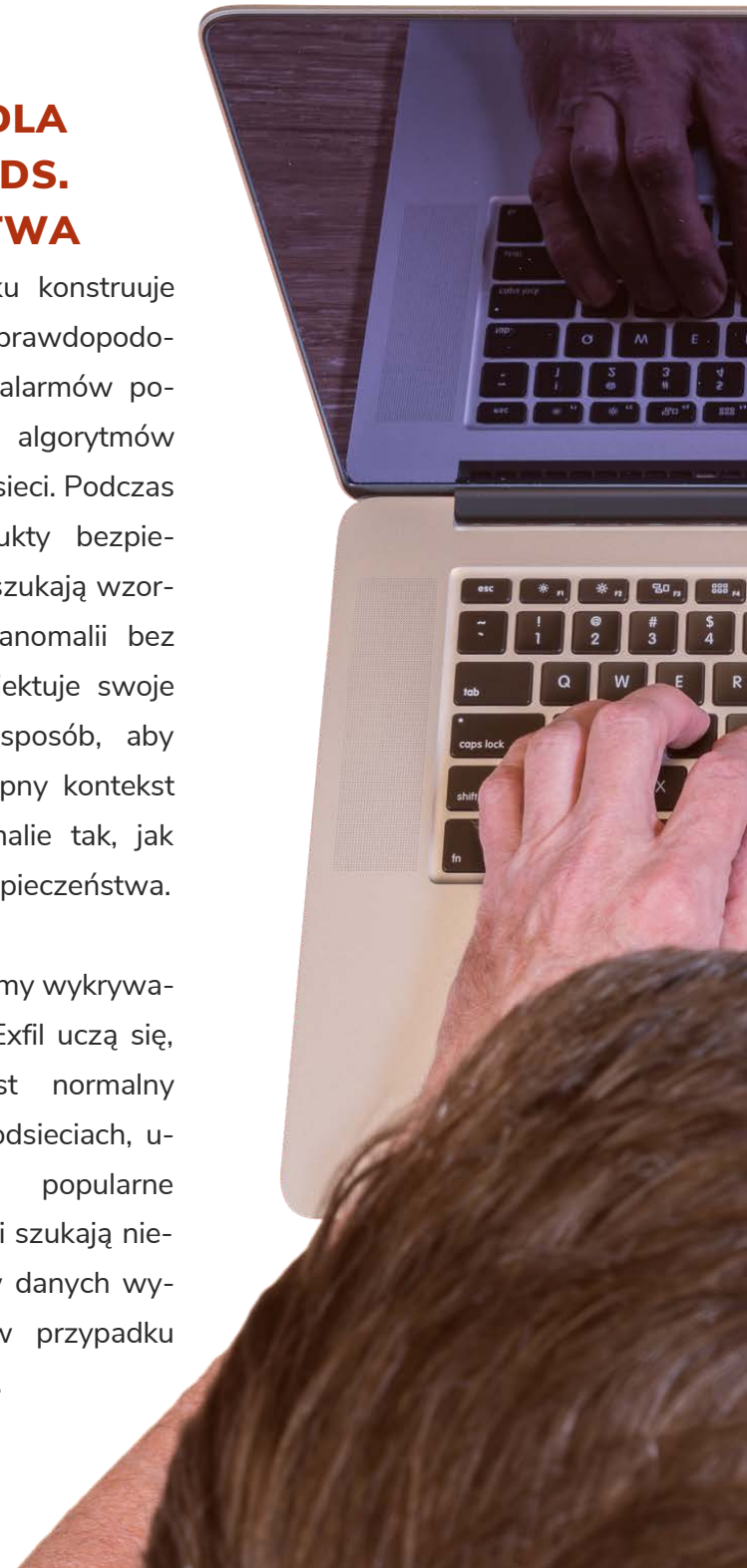
Istnieje wiele przyczyn problemów wynikających ze stosowaniem starszych rozwiązań bezpieczeństwa, ale w dużej mierze sprowadzają się one do:

- uproszczonych reguł dopasowania zdarzenia czy anomalii powodujących fałszywe alarmy,
- niezdolności do wykorzystania wskazówek kontekstowych w sieci w celu poprawy skuteczności,
- skupienie się wyłącznie na wykrywaniu, bez pomysłu jak efektywnie pogrupować zdarzenia, tak, aby analityk mógł skupić się na rzeczach, które faktycznie wymagają jego uwagi.

UŁATWIENIA DLA ANALITYKÓW DS. BEZPIECZEŃSTWA

Vectra AI od początku konstruuje detektory eliminujące prawdopodobieństwo fałszywych alarmów poprzez wzmocnienie algorytmów wiedzą o kontekście z sieci. Podczas gdy tradycyjne produkty bezpieczeństwa sieciowego szukają wzorca lub statystycznej anomalii bez kontekstu, Vectra projektuje swoje rozwiązania w taki sposób, aby wykorzystywały dostępny kontekst i identyfikowały anomalie tak, jak zrobiłby to analityk bezpieczeństwa.

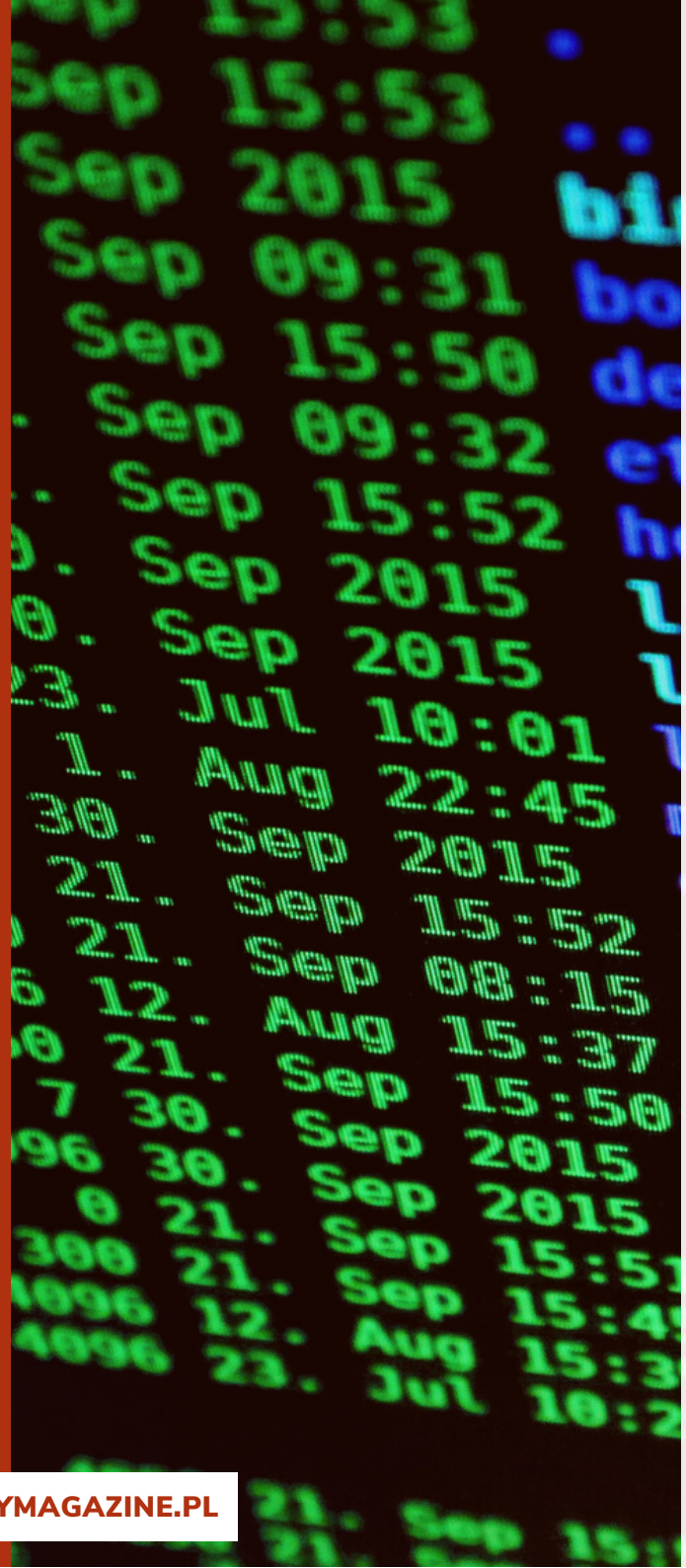
Na przykład, mechanizmy wykrywania Smash and Grab Exfil uczą się, jaki ruch danych jest normalny w poszczególnych podsieciach, uwzględniają witryny popularne w danym środowisku i szukają nietypowych przepływów danych wychodzących, nawet w przypadku zaszyfrowanego ruchu.



Następnie narzędzie Vectry koreluje wykrycia z podmiotami typu Host i Account, ucząc się archetypu i identyfikując każdy obiekt. W kolejnym kroku nadaje wykrywanym obiektom priorytety i tworzy ranking umożliwiający analitykom podjęcie działań.

Obszarem, który Vectra chciała poprawić, było radzenie sobie z poprawnie wykrytymi 'True Positives'. Wynikało to z tego, że nie wszystkie są złośliwe. Można również niezawodnie wykryć aktywność, w której zachowanie jest takie, jak mówi system; w kontekście, w którym zdarzenie ma miejsce, może to być raczej łagodny True Positive niż złośliwy True Positive. Na przykład, niektóre produkty antywirusowe osadzają wyszukiwane sumy kontrolne plików w zapytaniach DNS do dostawcy AV. To zachowanie może wyglądać bardzo podobnie do kanału dostępu typu Command-and-Control, który koduje dane w pakietach DNS, i tak właśnie jest. Jednak faktem jest, że choć jest to prawdziwy tunel DNS, nie jest on złośliwy, a raczej łagodny. Częścią naszej filozofii jest to, że zapewniamy wgląd w te wysokiej jakości wykrycia zachowań i metod atakujących, ale równoważymy to poprzez nadawanie priorytetu wysoce wiarygodnym, skorelowanym detekcjom na poziomie hosta lub konta w celu zwrócenia uwagi użytkownika.

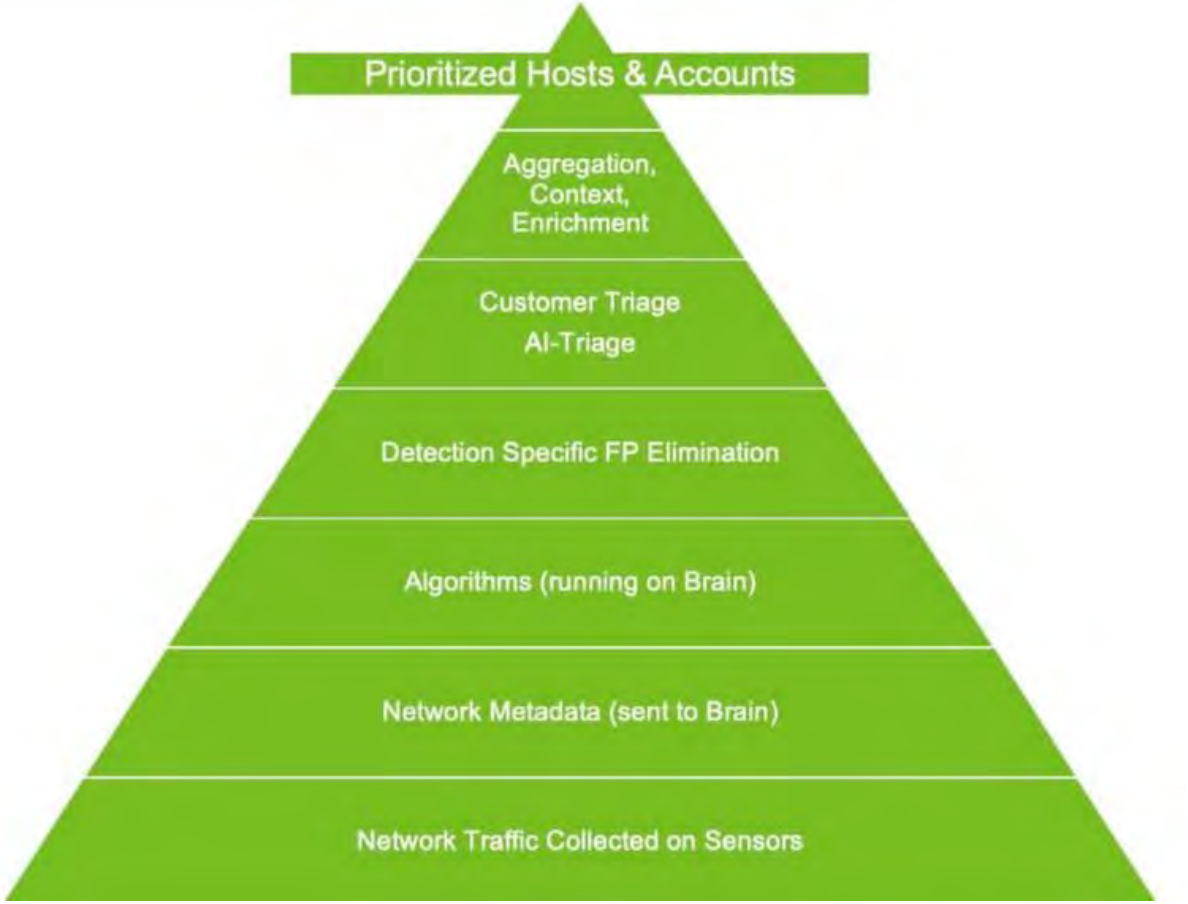
TO SKŁONIŁO PRZEDSTAWICIELI FIRMY DO ZASTANOWIENIA SIĘ, CZY ISTNIEJE SPOSÓB, W JAKI MOŻNA ZASTOSOWAĆ NIEKTÓRE Z TYCH SAMYCH TECHNIK, KTÓRE WYKORZYSTYWANE BYŁY DO ZASILANIA ALGORYTMÓW UCZENIA MASZYNOWEGO / SI, ABY POMÓC W ROZRÓŻNIANIU ZŁOŚLIWYCH I ŁAGODNYCH TRUE POSITIVES? CELEM BYŁO WYELIMINOWANIE KONIECZNOŚCI ANALIZOWANIA PRZEZ KLIENTÓW ŁAGODNYCH ZGŁOSZEŃ, PRZY JEDNOCZESNYM NADAWANIU PRIORYTETU TYM NIEBEZPIECZNYM. TAK NARODZIŁA SIĘ AI-TRIAGE.



Podobnie jak w przypadku procesu tworzenia detekcji, Vectra AI dodała możliwości AI-Triage, analizując najpierw metodologię, którą analitycy stosują do rozwiązywania tych problemów. Następnie przeszkoliła system SI, aby pomógł zautomatyzować rozwiązywanie scenariuszy o najwyższym stopniu zaufania.

JAK DZIAŁA AI-TRIAGE?

Wbudowana w platformę Vectra funkcja AI -Triage działa poprzez automatyczną analizę wszystkich aktywnych detekcji w systemie, wykorzystując kontekst z poszczególnych detekcji, jak również podobieństwa między detekcjami w celu poszukiwania przypadków łagodnych pozytywów, które możemy automatycznie rozwiązać w imieniu klienta. Na przykład, jeśli widzimy dziesiątki punktów końcowych generujących tę samą detekcję ukrytego tunelu HTTPS do tego samego miejsca docelowego, w ciągu co najmniej 14 dni, bez innych wskaźników naruszenia zabezpieczeń, możemy zidentyfikować to jako łagodny wynik pozytywny. AI-Triage automatycznie utworzy regułę segregacji w imieniu klientów, nie wymagając czasu od analityka. Jeśli analityk chce przejrzeć nowe reguły, może je nadal zmodyfikować w ramach platformy, ale nie jest to wymagane i nie wpływa na ocenę hosta ani konta.

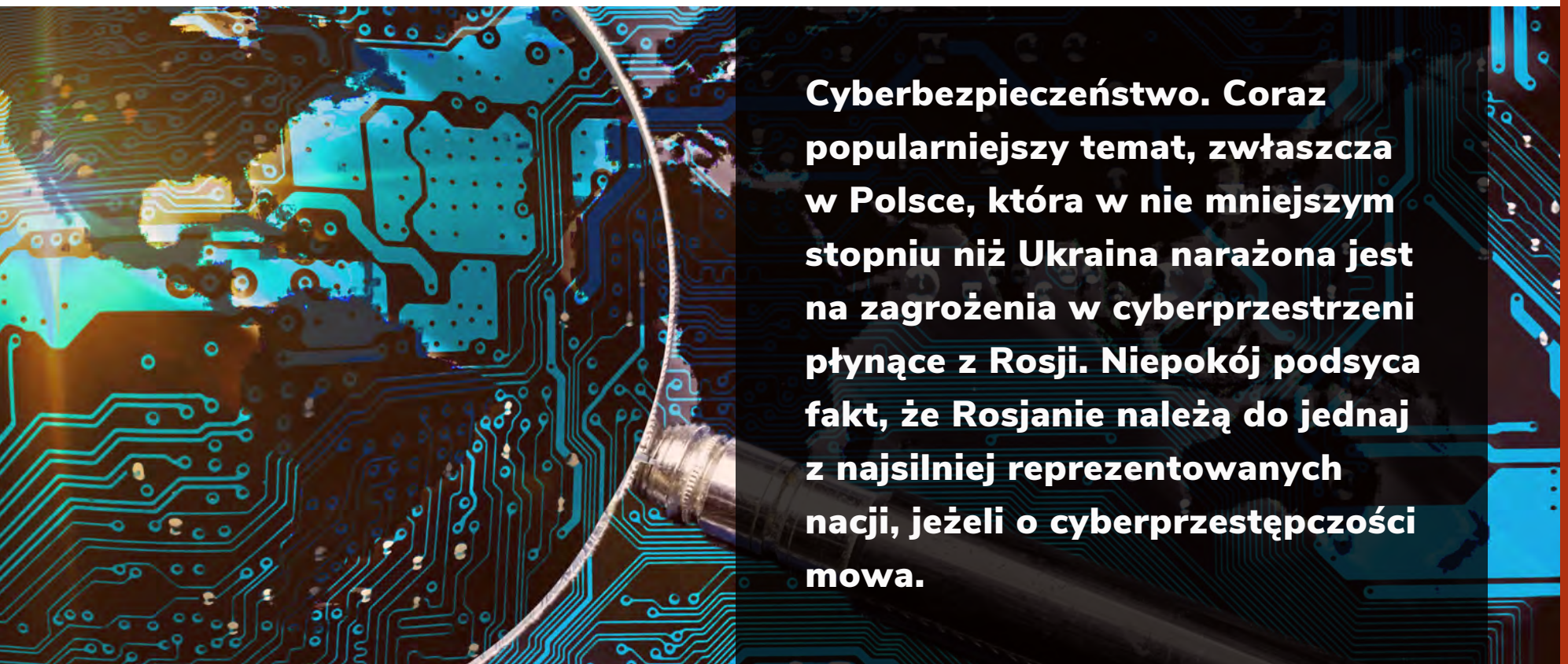


Początkowo wprowadzono obsługę AI-Triage dla wykryć opartych na C2 i Exfil, a w nadchodzącym wydaniu sprawdzony szkielet wykorzystano, aby rozszerzyć AI-Triage na wykrycia ruchu poprzecznego (Lateral). Okazało się, że AI-Triage zmniejsza o ponad 80% liczbę wykryć, które musiałby zbadać analityk, co oznacza, że więcej czasu można poświęcić na zdarzenia wymagające uwagi analityka.

Wszystkie możliwości, które daje AI-Triage można aktywować jednym kliknięciem - nie są wymagane żadne dostrajania ani administracja ze strony klienta. Aby włączyć funkcję, wystarczy przejść do Ustawień, wybrać funkcję AI-Triage i włączyć ją, po czym AI-Triage zacznie działać, aby zidentyfikować łagodne, faktyczne zagrożenia i dokonać ich selekcji.

CYBERSECURITY MADE IN POLAND

Michał Łęcki
Elmark Automatyka



Cyberbezpieczeństwo. Coraz popularniejszy temat, zwłaszcza w Polsce, która w nie mniejszym stopniu niż Ukraina narażona jest na zagrożenia w cyberprzestrzeni płynące z Rosji. Niepokój podsyca fakt, że Rosjanie należą do jednaj z najsilniej reprezentowanych nacji, jeżeli o cyberprzestępczości mowa.

Ale to nie "zwykły Kowalski" powinien czuć się zagrożony, a ci, którzy na co dzień zajmują się elementami infrastruktury kluczowej w sektorze OT. Jak zatem prezentuje się (cyber)bezpieczeństwo naszego przemysłu i jak wypadamy na tle pozostałych krajów, lub inaczej mówiąc, średniej globalnej?

CYBERBEZPIECZEŃSTWO W POLSCE

To pytanie zadaliśmy sobie (oraz innym) nieco wcześniej niż 24 lutego. Ciekawi tego, jak prezentuje się polski przemysł w ramach cybersecurity postanowiliśmy przeprowadzić badanie. Od lipca do grudnia 2021 udostępniliśmy anonimową ankietę, celem której było rozpoznanie polskiego rynku cyberbezpieczeństwa. Odpowiedzi udzieliło nam ponad 130 specjalistów. Śmiało możemy powiedzieć, że badaniem udało nam się objąć pełne spectrum przemysłu, począwszy od małych firm zatrudniających poniżej 10 pracowników aż po największe organizacje skupiające powyżej 250 osób.

13. Rozmiar przedsiębiorstwa (na podstawie liczby zatrudnionych osób, bez względu na rodzaj umowy)

Odpowiedź	%	Liczba odpowiedzi
Duże (> 250)	31.21%	44
Średnie (< 250)	19.86%	28
Małe (< 50)	18.44%	26
Mikro (< 10)	30.50%	43

Zebrane przez nas dane zestawiliśmy z raportem opublikowanym przez firmę Claroty State of Industrial Cybersecurity 2021 oraz SANS 2021 Survey: OT/ICS Cybersecurity.

Już na pierwszy rzut oka obserwowalna jest pewna niedojrzałość naszego rynku OT w zakresie jego cyberbezpieczeństwa.

Ankietowani zapytani o to, kto w ich organizacji odpowiada za bezpieczeństwo sieci OT/ICS w przeważającej większości wskazali Dział IT. Natomiast nie to o naszej niedojrzałości świadczy.

Jedynie 25% zadeklarowało, iż ma specjalny zespół powołany do tego celu.

16. Kto w przedsiębiorstwie odpowiedzialny jest za bezpieczeństwo sieci OT

Odpowiedź	%	Liczba odpowiedzi
Inżynier utrzymania ruchu / automatyk	18.44%	26
Dział IT	40.43%	57
Dedykowany inżynier/zespół ds. cyberbezpieczeństwa	24.82%	35
Nie wiem	13.48%	19
Ktoś inny. Kto? — odpowiedzi	2.84%	4

W ujęciu globalnym, idąc za danymi firmy Claroty, ponad 60% organizacji posiada dedykowaną temu zadaniu komórkę w swojej firmie. Natomiast podobnie jak na naszym rodzimym rynku w około 20% organizacji za bezpieczeństwo odpowiada dział Utrzymania Ruchu, a w ok. 10% pracownicy nie wiedzą, kto jest odpowiedzialny za to zadanie.

Ta swoista niedojrzałość naszego rynku objawia się również w innej kwestii. W ujęciu globalnym za największe zagrożenie organizacje wskazują ataki typu **ransomware.** Zwłaszcza w dobie popularyzacji ataków typu RaaS (czyli de facto hackowania na żądanie), które znalazły swoje „zyskowne" miejsce w przestrzeni OT. Jednak polscy przedsiębiorcy jako główne zagrożenie wskazują w dalszym ciągu ludzi.

Blisko 83% respondentów wskazało tę właśnie odpowiedź. Ma to swoje uzasadnienie, ponieważ **poziom kompetencji w zakresie cyberbezpieczeństwa jest, niestety, w dalszym ciągu dość niski.** Jest to rezultat długu technologicznego, który w dalszym ciągu posiadamy. Wielu spośród automatyków nie dopuszcza nawet do siebie myśli, że może zostać zaatakowanymi, ponieważ sieci OT to w przeważającej liczbie układy zamknięte, które nie mają wyjścia „na świat".

Tym samym jedynym źródłem ataku może być niekompetentny pracownik lub tzw. „man in the middle". To jednak złudne myślenie, ponieważ pandemia Covid-19 nieco zmieniła podejście do świadczenia usług serwisowych

i zdalny dostęp w przemyśle stał się czymś bardzo powszechnym, co całkowicie podważa podawane wcześniej argumenty.

Najciekawszym jednak pytaniem, bez którego takie badanie nie mogło się obejść było: "Czy w ciągu ostatnich 12 miesięcy w przedsiębiorstwie zdarzył się indcydent związany z cyberbezpieczeństwem?" I tu rezultaty absolutnie nas zaskoczyły. Z przedstawionych odpowiedzi, wynika, że albo jesteśmy fantastycznie przygotowani, albo... właśnie... Wnioski nasuwają się same. Prawdopodobnie część z osób, które wskazały odpowiedź NIE, powinno jednak wskazać odpowiedź NIE WIEM.

Dane z raportów globalnych by na to wskazywały. Claroty jest w tym aspekcie bezwzględne.

Wedle ich danych ponad 80% organizacji padło ofiarami ataku, z czego 47% z nich miało bezpośredni wpływ na funkcjonowanie sieci OT oraz systemów ICS. SANS podaje nieco mniej apokaliptyczne dane, jednak w dalszym ciągu jedynie 12% respondentów jest przekonanych, że definitywnie nie zostało zaatakowanych.

17. Czy w ciągu ostatniego roku w przedsiębiorstwie zdarzył się incydent związany z cyberbezpieczeństwem?

Odpowiedź	%	Liczba odpowiedzi
Tak	26.24%	37
Nie	56.03%	79
Nie wiem	17.73%	25

CZY POLSKI PRZEMYSŁ JEST CYBERBEZPIECZNY?

Nie ma jednoznacznej odpowiedzi na to pytanie. Ustawa o Krajowym Systemie Cyberbezpieczeństwa wymogła wdrożenie wielu polityk, zwłaszcza na operatorach usług kluczowych. Organizacje, od których zależy bezpieczeństwo kraju są dobrze przygotowane pod wieloma względami.

Faktem jest jednak, że polski przemysł dostrzega problem i ma świadomość tego, że cyberbezpieczeństwo, to jedna z kluczowych kompetencji jaką powinni nabyć pracownicy.

Zatem ku pokrzepieniu serc ostatnie zadane przez nas pytanie. Przedsiębiorcy zapytani o to, czy planują przeszkolenie pracowników pod kątem cyberbezpieczeństwa w przeważającej większości odpowiedzieli, że tak (58%).

JAKUB JACEK

Jak zwiększyliśmy sprzedaż z reklamy na Facebooku 13 razy w ciągu 4 miesięcy

W ciągu czterech miesięcy od daty rozpoczęcia ścisłej kampanii sprzedażowej, uzyskaliśmy **ponad 13 000% ROAS**u.

Jak do tego doszliśmy, z jakich technik skorzystaliśmy i w jaki sposób konfigurowaliśmy techniczne i wizualne aspekty kampanii reklamowej dla polskiej marki odzieżowej?

Wyjaśniamy w artykule!

PRZECZYTAJ CASE STUDY

SPRAWDŹ OFERTĘ

Meta
Business Partner

Komu już pomogliśmy

Baltic Alians

PRAKreacja.pl
prawo dla kreatywnych

sam
WYDAWNICTWO

dollo

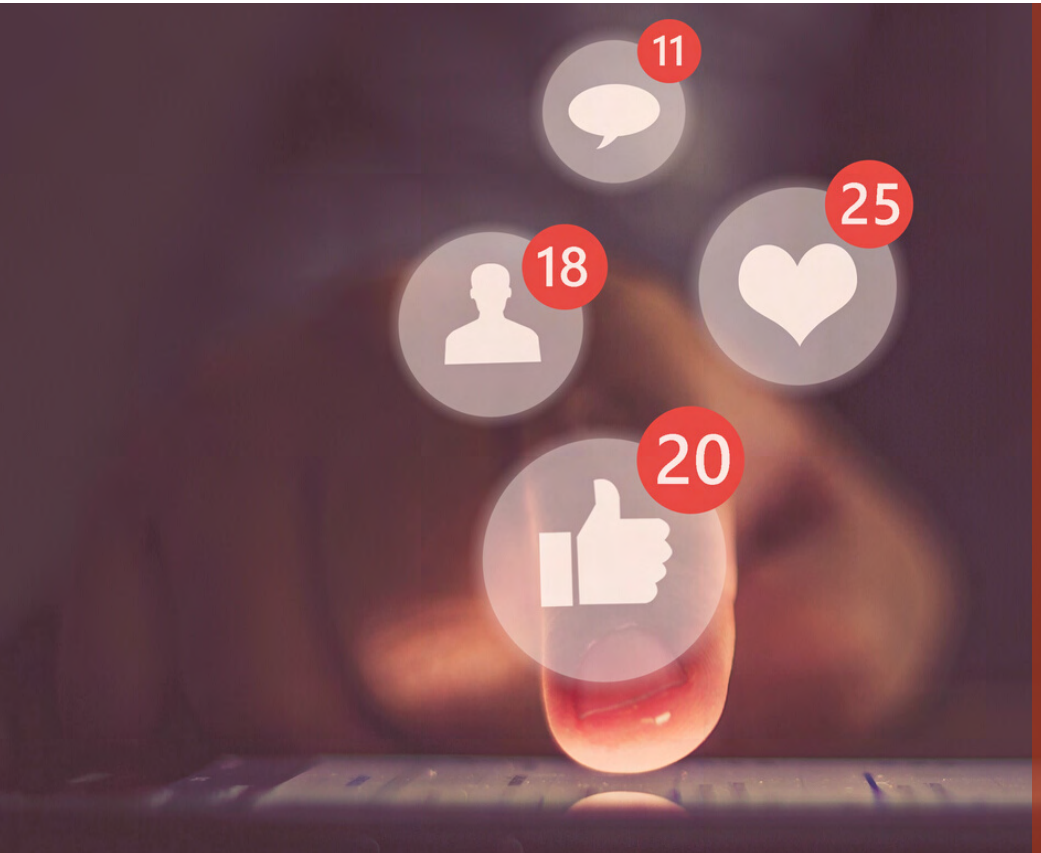
vippi
DESIGN

BUKEBUK

BY YOUR SIDE

BEZPIECZNIE W MARKETINGU ONLINE?

Jakub Jacek
jakubjacek.pro



Wykradzione środki reklamowe, ujawnione dane osobowe oraz przejęte konta administratorów to ostatnimi czasy plaga mediów społecznościowych. Ochronę przed tymi zagrożeniami można jednak prosto i łatwo sobie zapewnić. Jak chronić bezpieczeństwo działań marketingowych w sieci?

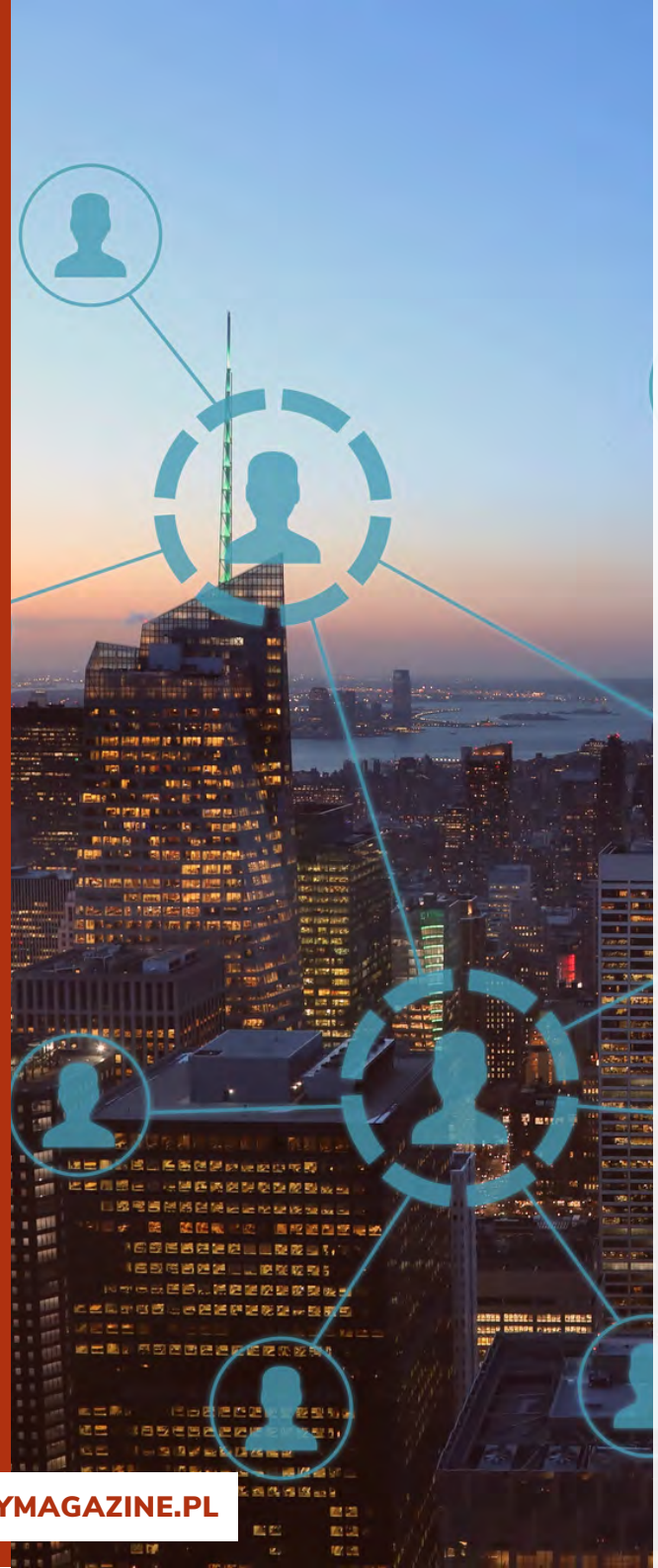
BRAK ZABEZPIECZEŃ MA SWOJĄ CENĘ

Postęp technologiczny spowodował, że coraz więcej aktywności biznesowych przenosi się do sieci. Aby korzystanie z dobrodziejstw online'u było w pełni komfortowe, konieczne jest wdrożenie podstawowych zasad bezpieczeństwa.

Te ważne są przede wszystkim, jeśli korzysta się z mediów społecznościowych. Na tych platformach najczęściej dochodzi do ataków hakerskich, które przyjmują formę przejęcia konta, kradzieży danych osobowych, czy wysyłania fałszywych informacji i linków phishingowych, które mogą skutkować „wyczyszczeniem" firmowej karty bankowej do granic jej limitów.

Koszty włamań na konta mediów społecznościowych są więc wysokie przede wszystkim dla firm. Wiążą się zarówno z utratą zaufania klientów i kontrahentów, jak i stratami finansowymi oraz nierzadko także konsekwencjami prawnymi. Aby się uchronić przed takimi następstwami, warto wdrożyć zasady zwiększające bezpieczeństwo działań marketingowych.

Wbrew powszechnemu przekonaniu zastosowanie zasad bezpieczeństwa nie jest trudne, czasochłonne ani kosztowne. Korzyści z ich wdrożenia są natomiast znaczne, a do najważniejszych z nich należy ograniczenie kosztów i potencjalnych problemów finansowych (kary nałożone przez prezesa UODO za wycieki danych osobowych), prawnych



(konieczność korzystania z pomocy prawnej przy oskarżeniach o zaniedbania dotyczące danych osobowych), wizerunkowych (utrata zaufania w oczach klientów i partnerów biznesowych) i osobowych (konieczność zaangażowania pracowników lub zewnętrznych firm, które naprawią sytuację).

JAK CHRONIĆ FIRMOWE ZASOBY ONLINE?

Najważniejszym krokiem jest ustalenie bezpiecznego sposobu logowania do konta. Podstawą jest oczywiście **silne hasło** – zawierające minimum 8 znaków i składające się z wymieszanych małych i dużych liter, cyfr
i znaków specjalnych, zmieniane minimum raz w roku oraz stosowane tylko do jednego konta, na jednym portalu. Takie hasło będzie trudno złamać, a w przypadku jego ewentualnego pozyskania, haker nie uzyska od razu dostępu do wszystkich kanałów komunikacji marki.

Silne i skomplikowane hasło często jednak jest niewystarczające. Aby chronić firmowe konta na mediach społecznościowych, obowiązkowa jest **weryfikacja dwuskładnikowa**. Polega ona na konieczności wprowadzania dodatkowego, jednorazowego kodu zaraz po podaniu hasła głównego do konta. Kod wysłany jest najczęściej SMS-em na wskazany numer telefonu lub jest generowany w aplikacjach mobilnych takich jak Google Authenticator lub Yubico Authenticator.

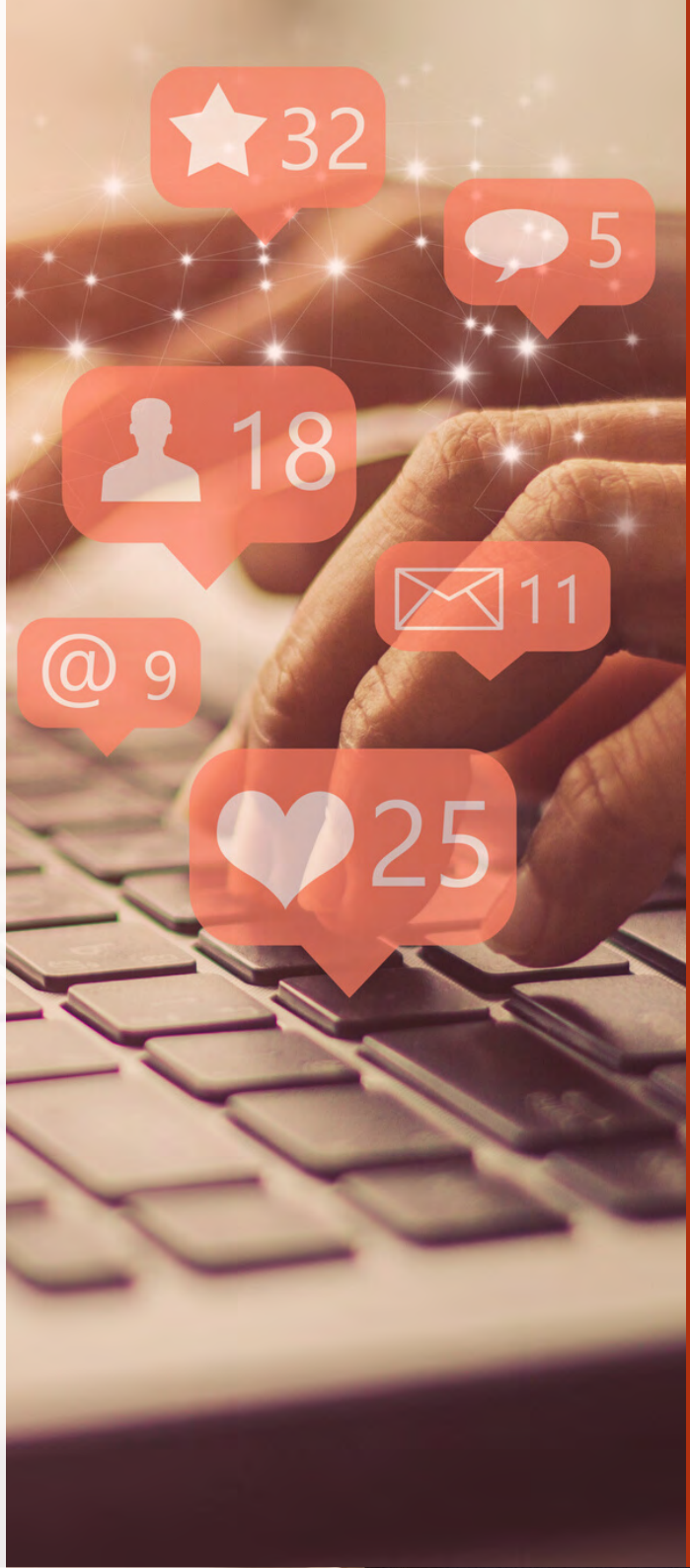
Warto jednak zaznaczyć, że tak wysłane kody równie łatwo przechwycić, co wygenerować. Hakerzy wykorzystują do tego np. phishing, czyli podszywanie się pod inną osobę lub instytucję w celu wyłudzenia poufnych informacji, zainstalowania szkodliwego oprogramowania lub zmuszenia do danego działania.

W praktyce firmy padające ofiarą phishingu, otrzymują np. maila przekierowującego do strony wyglądającej dokładnie tak samo jak ta do logowania na dany portal i sama zdradza hasło i login (oraz coraz częściej także jednorazowy kod Dwuskładnikowego Uwierzytelniania).

Zasady bezpieczeństwa nakazują więc powstrzymanie się od klikania w linki i załączniki wyglądające podejrzanie, zawierające szokujące lub kontrowersyjne treści lub po prostu budzące emocje. Ponadto powszechnie stosowaną metodą kradzieży kodów jednorazowych jest też SIM spoof i SIM swap.

Chcąc ochronić się przez wspomnianymi atakami, warto zainwestować w **klucz U2F** (Universal 2nd Factor). Znajduje się on na **fizycznym urządzeniu przypominającym pendrive** z portem USB. Przejęcie tego urządzenia przez hakerów jest niemal niemożliwe (ponieważ wiązałoby się ono z fizycznym wyrwaniem klucza z dłoni ofiary), przez co rezygnują oni z włamań i przejęć kont zabezpieczonych takim tokenem. **Korzystanie z klucza U2F w 100% ochroni firmę** przed phishingiem, a także uprości i przyspieszy logowanie do portali. Klucz U2F można wykorzystać do logowania się do serwisów jak: **Facebook, Instagram, Gmail, Microsoft, Youtube, DropBox czy Twitter, a także do bankowości internetowej.**

Klucz U2F nie jest już obecnie drogim zabezpieczeniem dostępnym wyłącznie dla najbogatszych, dlatego powinien być w niego zaopatrzony każdy administrator posiadający dostęp do kluczowych zasobów cyfrowych w firmie. W ostatnich latach ceny tego typu urządzeń spadły i można je kupić u autoryzowanych partnerów.



JAK PRZYŚPIESZYĆ REAGOWANIE W SYTUACJACH KRYZYSOWYCH?

Często jednak, nawet przy najskuteczniejszych zabezpieczeniach, zawieźć może najdoskonalsza „maszyna" jaką znamy – człowiek. Wdrożone zasady bezpieczeństwa powinny więc nie tylko zapobiegać, ale również umożliwić **szybkie zidentyfikowanie problemu**, znalezienie jego źródła i zareagowanie.

Kluczem do sprawnego rozwiązania komplikacji będzie **porządek na kontach**, menedżerach i systemach zarządzania uprawnieniami. Utrzymywany powinien on być w pełnym zakresie prowadzonych działań przez wszystkie zaangażowane w proces osoby. **Spójne nazewnictwo i uporządkowanie struktury** w zakresie kampanii, zestawów reklam, kont reklamowych i analitycznych czy skonfigurowanych metod płatności pozwoli niemal automatycznie zorientować się, że dochodzi do nieprawidłowości, a także błyskawicznie odnaleźć ich przyczynę.

W dbaniu o bezpieczeństwo konta firmowego na Facebooku pomoże też **ostrożność w nadawaniu dostępów.** Pamiętajmy o przydzielaniu ich przy dokładnej weryfikacji, jaki stopień uprawnień jest potrzebny danemu pracownikowi. Regularnie należy również kontrolować, czy dostęp do Fanpage'a, czy Instagrama mają wyłącznie osoby zatrudnione i odpowiedzialne za działania komunikacyjne w social media firmy.

Uprawnienia znajdujące się w niepowołanych rękach np. zwolnionych pracowników znacząco obniżają bezpieczeństwo konta oraz nierzadko skutkują całkowitą utratą kontroli nad kluczowymi w obecnych czasach kanałami komunikacji marki.

BEZPIECZEŃSTWO PRZY WSPÓŁPRACY Z PODWYKONAWCAMI

Firmy korzystające z pomocy zewnętrznych agencji reklamowych lub freelancerów stosować powinny się do wszystkich wyżej wymienionych zasad oraz dodatkowo zadbać także o kwestie formalne.

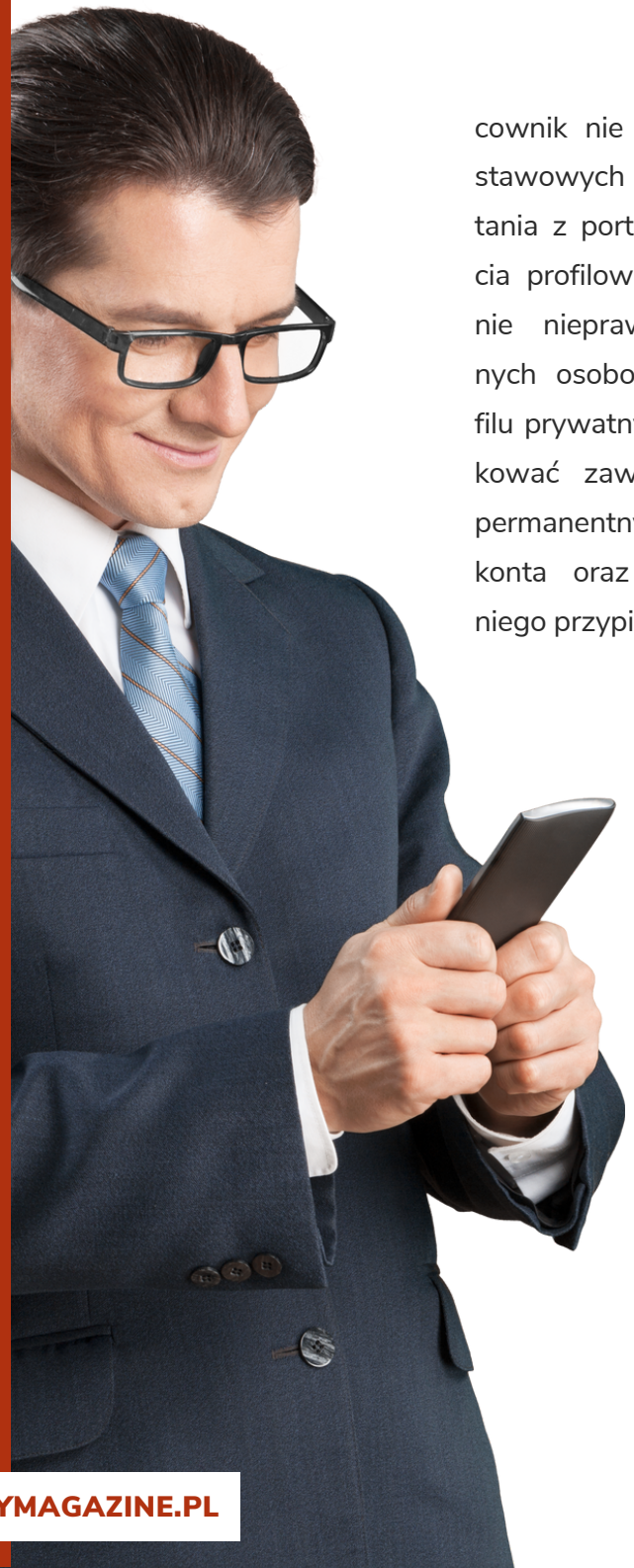
Podstawą współpracy zawsze musi być spisana umowa, w której ujęte zostaną wszystkie kluczowe kwestie takie jak np. prawa autorskie do grafik czy tekstów. W dokumencie nie może również zabraknąć paragrafów mówiących, jakie mają być

dokładne efekty współpracy (najlepiej ująć je w wymiarze liczbowym lub na przykładach realizacji) i w jaki sposób mają one być rozliczane. Takie zapisy pozwolą uniknąć późniejszych sporów na linii firma – agencja reklamowa lub firma - freelancer.

Prawa autorskie, efekt współpracy oraz wysokość i forma rozliczania to elementy, które znajdują się w większości umów. Mniej powszechne jest zapisywanie w nich, jak dokładnie ma wyglądać współpraca. Tymczasem jest to **kluczowe dla bezpieczeństwa kont reklamowych firmy**. Chcąc je chronić, przedsiębiorstwo **nie powinno się godzić na podawanie haseł**, zbędnych dostępów, **numerów kart** kredytowych podpinanych do kont reklamowych. Wynika to z tego, że im więcej osób pozyska informacje poufne, tym większe ryzyko ich wycieku (dodatkowo podawanie takich informacji osobom trzecim jest najczęściej niezgodne z polityką portalu lub banku).

Partnerom biznesowym dostępy nadawać powinno się zgodnie z regulaminem Facebooka oraz dobrymi zwyczajami tj. poprzez Business Menagera, a nie podając bezpośrednie hasło do logowania.

Od agencji należy też wymagać, aby każda osoba przydzielona do obsługi Facebooka czy Instagrama **pracowała na swoim prawdziwym koncie personalnym**, które będzie posiadało autentyczne zdjęcie profilowe, prawdziwe imię i nazwisko, dane kontaktowe oraz uruchomioną **dwuskładnikową weryfikację**. W ten sposób firma zyskuje pewność, że **współpracuje z realną osobą**, dzięki czemu będzie można łatwo rozpoznać ewentualne podszywanie się, a także dba o to, aby podwykonawca lub pra-



cownik nie naruszył podstawowych zasad korzystania z portalu (brak zdjęcia profilowego lub podanie nieprawdziwych danych osobowych na profilu prywatnym może skutkować zawieszeniem lub permanentnym usunięciem konta oraz zasobów do niego przypisanych).

ZABEZPIECZENIE PRYWATNEGO KONTA W SOCIAL MEDIA

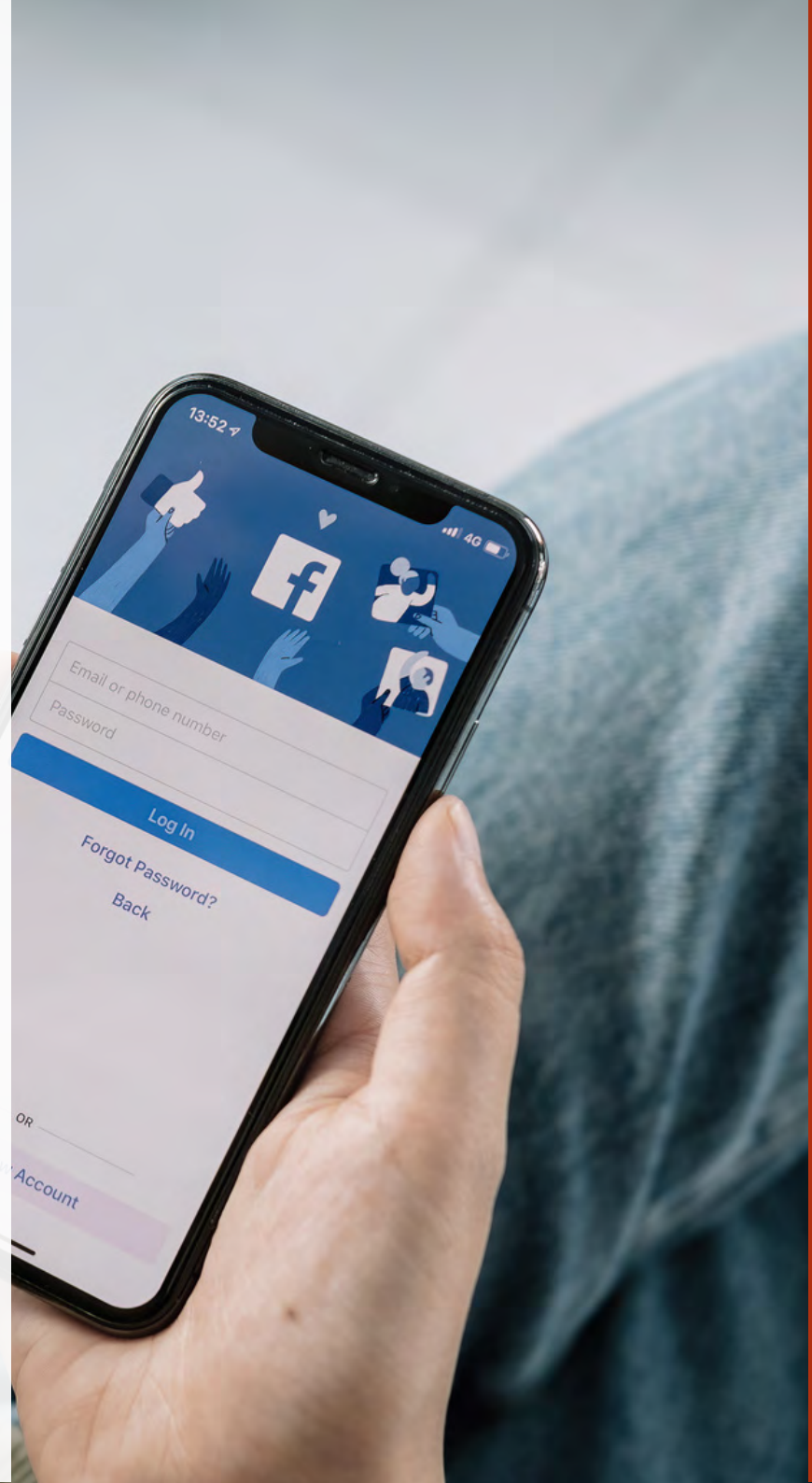
Przejmowanie kont to problem nie tylko stron firmowych w Social Media, ale także profili osób prywatnych. One również (szczególnie, gdy zarządzają zasobami firmowymi) powinny zabezpieczyć się poprzez wprowadzenie **uwierzytelniania dwuskładnikowego**.

Podobnie jak dla biznesu najskuteczniejszym wyjściem będzie nie kod jednorazowy, ale właśnie zaopatrzenie się w **prywatny klucz U2F**. Ponadto użytkownikom kont personalnych Meta oferuje również takie funkcje zabezpieczające jak: szyfrowanie wiadomości e-mail z powiadomieniami, powiadomienia o nierozpoznanych logowaniach czy stworzenie listy urządzeń, na których nie trzeba używać kodu do logowania (w myśl zasady bezpiecznie nie znaczy niewygodnie).

Omówione rozwiązania pozwolą skutecznie **chronić się przed atakami phishingowymi i włamaniami na konto** i to nie tylko na Facebooku, ale pozostałych platformach i systemach reklamowych.

W ochronie kont prywatnych zarządzających zasobami biznesowymi pomogą dodatkowo **regularne zmiany hasła** oraz upewnienie się, że podane w ustawieniach dane kontaktowe są poprawne.

Tak kompleksowo zabezpieczone zarówno konta administratora, jak i zasoby biznesowe gwarantują bezpieczeństwo oparte na trzech filarach – **profilaktyce, regularnej kontroli i alertowaniu** oraz reagowaniu w razie problemów. Dzięki nim nie musimy obawiać się o stan naszych zasobów firmowych teraz lub w przyszłości, a gdyby miał on ulec zmianie, zostaniemy o tym błyskawicznie poinformowani, co pozwoli na skuteczną reakcję.



Antywirus.com

30%
RABATU

KOD RABATOWY:

BFPSY30

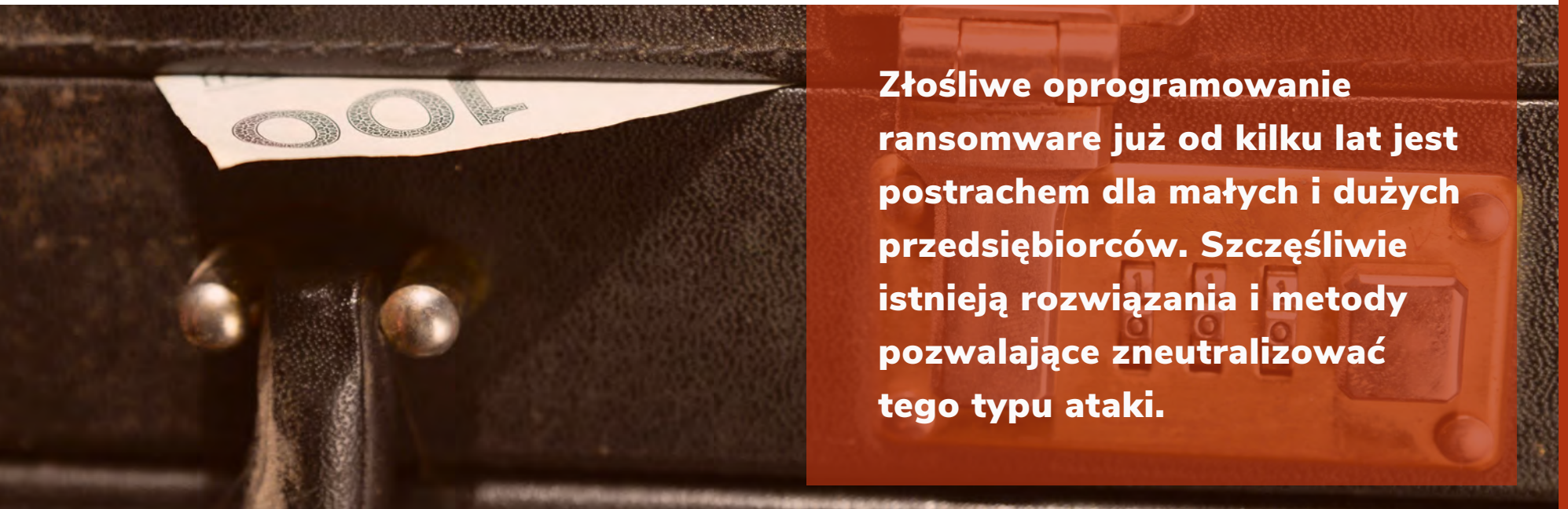
Cyberbezpieczny powrót do szkoły

Promocja dla czytelników Security Magazine:
do końca września wszystkie licencje
Bitdefender Family Pack z 30% rabatem

iOS

PIĘĆ TRUDNYCH LAT Z RANSOMWARE. JAK PRZECHYTRZYĆ CYBERGANGI?

Bartosz Adamczak
Marken - dystrybutor Bitdefender w Polsce



Złośliwe oprogramowanie ransomware już od kilku lat jest postrachem dla małych i dużych przedsiębiorców. Szczęśliwie istnieją rozwiązania i metody pozwalające zneutralizować tego typu ataki.

KONIEC LAT 80.

Pierwsze wzmianki o oprogramowaniu ransomware sięgają końca lat 80. Wówczas pojawił się program PC Cyborg, który szyfrował pliki, a następnie żądał od użytkownika „odnowienia licencji". W późniejszych latach pokazywały się różne szczepy ransomware'u, aczkolwiek punktem zwrotnym był ataki WannaCry oraz Petya przeprowadzone w 2017 roku. Oba złośliwe programy zdołały zaszyfrować dane setek tysięcy firm oraz użytkowników indywidualnych na całym świecie.

Oprogramowanie ransomware infekuje komputer, systemy sieciowe i przechowywane na nich dane. Następnie napastnicy szyfrują foldery z plikami typu dokument, arkusz kalkulacyjny, zdjęcia i wideo. Po zinfiltrowaniu maszyny, oprogramowanie kontaktuje się z centrum kontroli aby wygenerować klucz szyfrowania i zaszyfrować każdy istotny plik na komputerze wykorzystując złożony algorytm szyfrowania. Co istotne, od ubiegłego roku większość cybergangów stosuje tzw. podwójne wymuszenie. Oprócz tego, że hakerzy szyfrują dane, dodatkowo grożą ofierze, że jeśli nie zapłaci haraczu, upublicznią pozyskane informacje.

Ransomware jest rozpowszechniany za pomocą spamu czy ataków ukierunkowanych. Cybergangi chętnie sięgają po pierwszą z wymienionych opcji, szacuje się, że niemal połowę infekcji przeprowadzono za pomocą phishingu. Rozsyłane do potencjalnych ofiar e-maile zawierają zainfekowane pliki lub odnośniki do złośliwych witryn internetowych. Współcześni oszuści umiejętnie posługują się metodami inżynierii społecznej - wysyłane

przez nich wiadomości sprawiają wrażenie, że pochodzą od znajomych, przełożonych bądź zaufanych instytucji. Niestety, adresaci tego rodzaju spamu często połykają haczyk.

HORRENDALNE OKUPY: PŁACIĆ CZY NIE PŁACIĆ?

Gangi ransomware po wtargnięciu do sieci ofiary szyfrują pliki, a następnie żądają okupu za dostarczenie klucza deszyfrującego. Jednak problem polega na tym, że napastnicy nawet po zainkasowaniu haraczu, nie odszyfrowują danych. Ze statystki wynika, że dzieje się tak w co trzecim przypadku.

- *Opłaty za odszyfrowanie danych jakich żądają cyberprzestępcy są bardzo wysokie.* ***Światowa średnia wynosi w bieżącym roku około 210 tysięcy dolarów.*** *Choć oczywiście napastnicy stosują różne stawki, często odbiegającej od tej wartości. Znane są przypadki, że wielkie koncerny płaciły za klucz deszyfrujący kilka milionów dolarów. Na przeciwnym biegunie znajdują się użytkownicy indywidualni, od których cyberprzestępcy żądają od kilkuset do tysiąca dolarów* - tłumaczy **Mariusz Politowicz z firmy Marken, dystrybutora rozwiązań Bitdefender w Polsce.**

Jak wynika z danych firmy Coverware, w pierwszym kwartale bieżącego roku 46 proc. ofiar ataków ransomware zapłaciło przestępcom za odszyfrowanie plików. Większość specjalistów od cyberbezpieczeństwa jest przeciwna płaceniu haraczu, ponieważ wniesienie opłaty nigdy nie daje 100 proc. gwarancji odszyfrowania danych. Poza tym zachęca cyberprzestępców do przeprowadzenia kolejnych ataków, a także zasila ich budżety.

GANGI RANSOMWARE POLUJĄ NIE TYLKO NA BOGATYCH

Colonial Pipeline, Cisco, Nvidia, Knauf Gips, Canon, Volkswagen Group, Orange, Garmin to tylko kilka z wielu znanych koncernów, które padły ofiarą ataku ransomware. Jak się łatwo domyślić, duże firmy oraz instytucje są ulubionym celem cybergangów. Według danych telemetrycznych zebranych przez systemy Bitdefendera, napastnicy skoncentrowali się przede wszystkim na dochodowych terytoriach i branżach.

Ulubionym państwem gangów ransomware jest USA, gdzie skierowano 33 procent spośród wszystkich cyberataków.

Kolejne miejsca zajęły Niemcy z 12% udziałem, a następnie Ameryka Łacińska (11%). Włochy (11%), Wielka Brytania (8%). Napastnicy szczególnie upodobali sobie **sektor telekomunikacyjny**. W 2021 roku rozwiązania Bitdefender zablokowały 48% globalnych ataków ransomware w samej branży telekomunikacyjnej. **Media zajmują drugie miejsce (19%), za nimi uplasowały się takie branże jak: edukacja i badania (9 proc.), administracja (8%), technologia i usługi (1%.).**

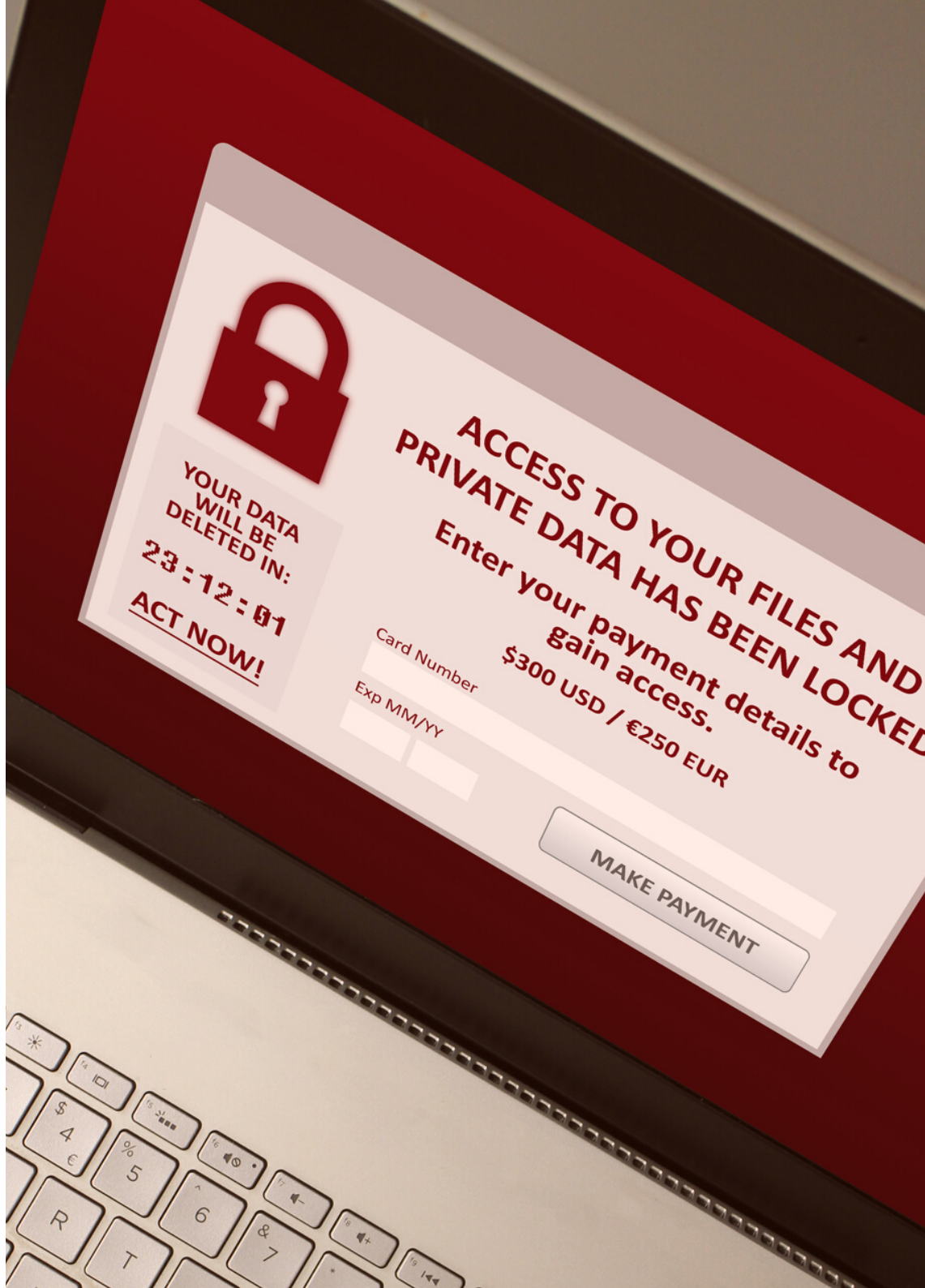
Nie oznacza to jednak, że właściciele małych i średnich firm mogą spać spokojnie. O ile duże gangi polują przede wszystkim na „grube ryby", o tyle początkujący hakerzy uderzają w mały biznes, a nawet gospodarstwa domowe.

Jest to możliwe, dzięki rozwojowi modelu „Ransomware as a Service". Najwięksi, doświadczeni twórcy malware'u udostępniają go sprzymierzonym podmiotom, pobierając w zamian prowizję. W rezultacie nieopierzeni napastnicy nie muszą posiadać obszernej wiedzy na temat technik ataków czy funkcjonowania sieci.

JAK SIĘ BRONIĆ?

Organizacje, chcąc chronić swoje dane, muszą posiadać przynajmniej podstawowe narzędzia bezpieczeństwa, takie jak oprogramowanie antywirusowe. W obecnych czasach każdy dostawca antywirusa deklaruje, że jego produkt stanowi skuteczną zaporę przed atakim ransomware. Jednak teoria często rozmija się z praktyką i sprytni hakerzy potrafią ominąć zabezpieczenia. Dlatego należy dokonywać racjonalnych wyborów i nie bazować wyłącznie na materiałach marketingowych producenta.

Cenną wskazówki dla osób poszukujących skutecznego zabezpieczenia przed oprogramowaniem ransomware są wyniki badania przeprowadzonego przez niezależny instytut badawczy AV-TEST. Analitycy przeprowadzili szczegółowe badania mające na celu sprawdzić skuteczność oprogramowania bezpieczeństwa pod kątem wykrywania ransomware'u. W teście brały udział między innymi Bitdefender Internet Security, Bitdefender Endpoint Security oraz Bitdefender Endpoint Security Ultra. Wszystkie trzy produkty wykazały się stuprocentową skutecznością w wykrywa-

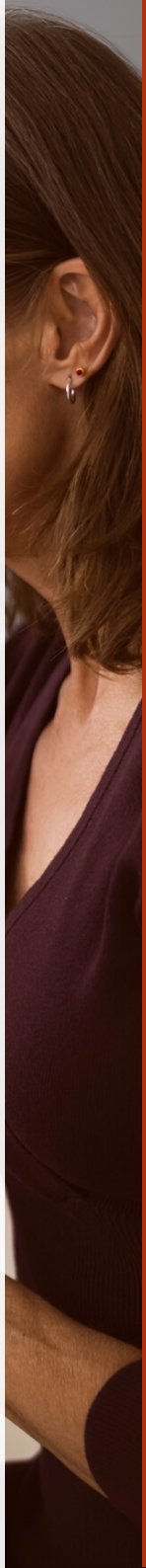


niu ransomware'u i otrzymały od AV-TEST maksymalną liczbę punktów.

Niezwykle ważna jest też aktualizacja podatnych komponentów infrastruktury. Działy IT muszą prowadzić stałą analizę i podatności. Nie jest to łatwy proces, zwłaszcza jeśli firma korzysta z tysięcy aplikacji. W tego typu przypadku warto skorzystać z odpowiedniego oprogramowania, wykonującego automatyczne aktualizacje.

Należy też dokładnie analizować konfigurację serwisów i aplikacji (eliminacja domyślnych ustawień, domyślnych haseł, zbędnych usług), a także ograniczyć do niezbędnego minimum używania kont serwisowych.

- *Organizacja chcąca powstrzymać gangi ransomoware musi zbudować politykę bezpieczeństwa infrastruktury, uwzględniającą proces pozyskiwania informacji o słabościach i wykonywania regularnych testów. Historia ransomware'u pokazuje, że napastnicy doskonale adaptują się do zmieniających się okoliczności i potrafią zaatakować w nowy i jeszcze bardziej dotkliwy sposób* - podsumowuje Mariusz Politowicz.



/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

CYBERSTRAŻNIK, BEZPIECZNIEJSZY BLOCKCHAIN I WIRTUALNY AUDYTOR

Redakcja
SECURITY MAGAZINE

Cyberbezpieczeństwo powinno być podstawą dla każdej firmy – niezależnie od tego, czy np. przechowuje i przetwarza dane swoich klientów, czy działa jedynie w obszarze produkcji. Wszystko, co podłączone do internetu – razem z urządzeniami IoT – jest narażone na cyberataki. Sprawdź, które startupy pomogą Ci zadbać o cyberbezpieczeństwo.

SAMURAI LABS – CYBERSTRAŻNIK

Cyberprzestępstwo wbrew pozorom to nie tylko ataki hakerskie. Polska policja rozróżnia kilka rodzajów cyberprzestępstw, tj. piractwo komputerowe, przestępczość związana z kartami magnetycznymi, oszustwa, fałszerstwa komputerowe, kradzieże impulsów telefonicznych, a nawet... rozpowszechnianie dziecięcej pornografii.
Z kolei na zachodzie często mówi się także o tzw. cyberbullyingu, do którego zalicza się m.in. trolling, choć nie zawsze jest on usankcjonowany.

Jednak patrząc w stronę wschodu – a konkretniej Indii – możemy się dowiedzieć, że ów trolling jest traktowany jak przestępstwo. I to m.in. właśnie przed takimi przypadkami pozwala nam się chronić technologia gdyńskiego startupu Samurai Labs. Spółka opracowała technologię z zakresu sztucznej inteligencji i uczenia maszynowego, która wykrywa i pomaga zapobiegać przemocy w sieci.

Dzięki tzw. cyberstrażnikowi możesz od razu wykryć destrukcyjne zachowania, takie jak trolling, groźby, wulgaryzmy, uwagi czy treści o charakterze seksualnym itd. Rozwiązanie Samurai Labs najzwyczajniej pomaga w moderacji społeczności na Twojej platformie, forum, portalu itp.

A o tym, jak destruktywne mogą być działania użytkowników, a zwłaszcza trolli i hakerów, wiele razy przekonał się Wykop.pl. Platforma regularnie jest atakowana przez cyberprzestępców, którzy hakują konta jej członków, po czym udostępniają w serwisie pornografię – niejednokrotnie dziecięcą.

Spółka chwali się m.in., że po wdrożeniu jej rozwiązania w jednej z najbardziej toksycznych internetowych społeczności (startup nie wskazał nazwy, być może obejmuje ich NDA), destrukcyjne zachowanie użytkowników zmniejszyło się o 45%.

Wśród klientów startupu znajdują się m.in. Hate Lab, Khoros, Inach, Webex, Heroo Mobile, a do partnerów zalicza się, chociażby Nvidia. Rozwiązanie startupu zostało także nagrodzone przez Gartnera czy CB Insights oraz opisane przez Business Insidera, BBC czy Forbesa.

ALEPH ZERO. "BEZPIECZNIEJSZY BLOCKCHAIN"

Aleph Zero to open-source'owa platforma blockchain, która ma być bezpieczniejszą i szybszą alternatywą dla tradycyjnego łańcucha bloków. Startup założyło w Krakowie czterech founderów – trzech Polaków i Amerykanin.

Aleph Zero jest zdecentralizowaną bazą danych, w której programiści mogą tworzyć swoje aplikacje. Nic jednak nie stoi na przeszkodzie, aby projekt ten wdrożyć do np. służby zdrowia, czy dokonywać na nim bezpiecznych transakcji – które są niezwykle szybkie i tanie.

System dostarczany przez krakowską spółkę jest odporny na tzw. problem bizantyńskich generałów (Byzantine Fault Tolerant). Oznacza to, że Aleph Zero jest utrzymywany przez duży komitet złożony z niezależnych węzłów. Dzięki temu system może funkcjonować nawet pomimo aktywnego ataku, który miałby doprowadzić do wyłączenia platformy lub wprowadzenia do niej błędów.

Startup umożliwia tworzenie inteligentnych kontraktów, decentralizację przechowywania plików w chmurze itd. itp. Z rozwiązania Aleph Zero korzystają głównie projekty blockchainowe, DeFi i kryptowalutowe, ale nie tylko. System krakowskiego startupu wdrożyła m.in. Linux Foundation.

SAGENSO – OCHRONA PRZED CYBERATAKAMI

Rzeszowski startup Sagenso jest znacznie bar-

dziej powiązany z tradycyjnie rozumianym cyberbezpieczeństwem. Spółka dostarcza narzędzia, które służą do wykonywania audytów bezpieczeństwa IT i wykrywania cyberzagrożeń. Pierwsze rozwiązanie nazywane jest **Telescope i funkcjonuje jako wirtualny menedżer i audytor.** Za jego pomocą można dokonywać samodzielnej analizy skuteczności praktyk i mechanizmów kontrolnych, ale też oceny poziomu bezpieczeństwa w zgodzie z regulacjami prawnymi.

Co ważne – **Telescope również samodzielnie rekomenduje gotowe propozycje ustawień procesowych i operacyjnych, więc nie tylko wykrywa nieprawidłowości, ale od razu pokazuje, co należy wdrożyć.**

Drugim narzędziem jest **CyberStudio**. To system automatyzujący proces wykrywania i usuwania cyberzagrożeń. **CyberStudio monitoruje i raportuje podatność na cyberatak – zarówno od strony organizacji, jak i pracowników.** Narzędzie ma dostarczać administratorom IT informacje o wyciekach danych, minimalizować ryzyko przejęcia kont pracowniczych i proponować usprawnienia w zakresie cyberbezpieczeństwa.

Startupów w obszarze cyberbezpieczeństwa jest, oczywiście, znacznie więcej. I to zarówno tych polskich, jak i zagranicznych. Jeśli prowadzisz własną firmę – powinieneś zadbać o jej odpowiednie zabezpieczenie. Niezależnie od tego, czy jest ona mała, średnia czy duża. Zagrożenia cyberprzestępczością będą bowiem, niestety, tylko wzrastać.

ABD

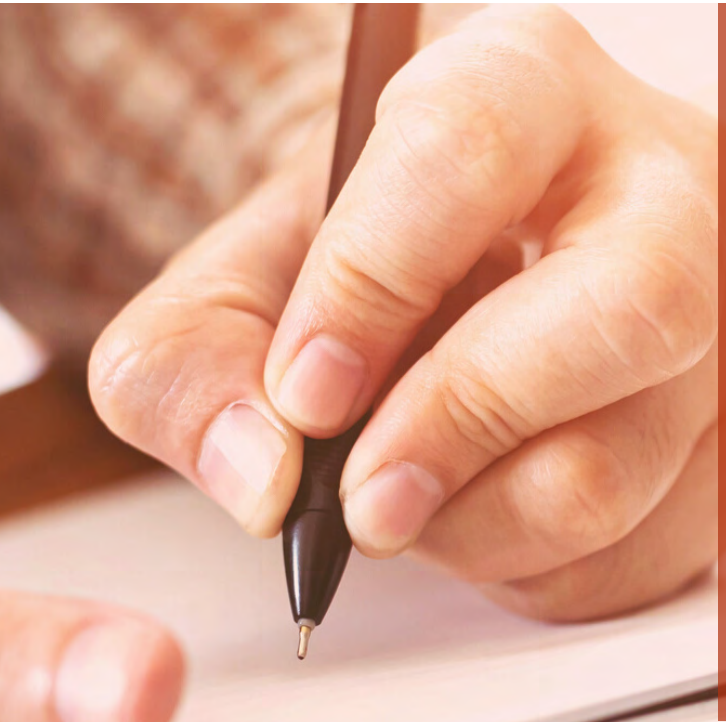
Agencja Bezpieczeństwa i Detektywistyki

SZKOLENIE MANAGER POSTĘPOWAŃ WEWNĘTRZNYCH W ZARZĄDZANIU KRYZYSOWYM

START
12.09

CZY ZARZĄDZANIA BEZPIECZEŃSTWEM FIRMY MOŻNA SIĘ NAUCZYĆ?

Maciej Zygmunt
Agencja Bezpieczeństwa i Detektywistyki



Oczywiście, że można. Jednak odpowiedź na pytanie jak to zrobić, nie jest już, niestety, taka prosta. Od trzydziestu lat zajmuję się sprawami związanymi z szeroko rozumianym bezpieczeństwem i jedno co mogę powiedzieć to, że większość uczy się tego najprostszą, ale najczęściej, wbrew powszechnej opinii mało efektywną, metodą czyli na własnych błędach.

NAUKA NA WŁASNYCH BŁĘDACH?

Uczyć się na błędach można i tak w Polsce nauki dotyczące zarządzania swoimi biznesami „pobiera" zdecydowana większość przedsiębiorców. Za taką naukę trzeba jednak, niestety, często bardzo słono zapłacić, a poza tym nauka taka może trwać bardzo długo, a jej elementy mogą być niekompletne i co najważniejsze oparte na „przestarzałym materiale".

Jeszcze w czasach, gdy przestępczością, w tym zorganizowaną przestępczością gospodarczą, zajmowałem się w strukturach Centralnego Biura Śledczego widziałem, że właśnie przestępcy należą do tych grup społecznych, które najszybciej przyswajają sobie wszelkie nowinki technologiczne i wykorzystują je zanim przeciętny człowiek zorientuje się, że takie możliwości w ogóle istnieją. To oni też bardzo często byli świetnie zorientowani we wszelkich zmianach i tzw. lukach prawnych.

Osoby, które prowadzą jakąkolwiek działalność gospodarczą doskonale wiedzą, ile niebezpieczeństw na nich czyha. I nie mówię tu tylko o tych zagrożeniach, za którymi stoją tzw. zawodowi przestępcy.

Czynników, które mogą mieć negatywny wpływ na tzw. ciągłość biznesową czyli strategiczną i taktyczną zdolność organizacji do przewidywania i reagowania na zdarzenia można wymienić wiele, ale podzielić je można na te wynikające z zagrożeń naturalnych (powodzie, trzęsienia ziemi, huragany itp.) oraz te, za którymi stoi działanie ludzkie (działania przestępcze, zaczynając od zwykłych kradzieży poprzez defraudacje, przyjmowanie korzyści materialnych po czyny tzw. nieuczciwej konkurencji, ataki terrorystyczne, cyberataki, strajki, ale także zwykłe niedbalstwo czy ludzkie błędy).

Gdyby przyjąć, że wystarczy tzw. uczenie się na własnych błędach, musielibyśmy przyjąć, że każdy przedsiębiorca jest równocześnie olbrzymim pechowcem i szczęściarzem, skoro miał okazję doświadczyć wszystkich tych wyżej wymienionych zdarzeń, a równocześnie przejść przez nie w stanie pozwalającym na to, aby wyniesione z nich doświadczenia móc wykorzystywać w dalszej działalności.

Nie jest moją intencją wywoływanie poczucia strachu i spowodowanie sytuacji, w której czytający ten tekst przedsiębiorca stwierdzi, że lepiej zawczasu zrezygnować z dalszej działalności, bo prędzej czy później czeka na niego katastrofa.

Czy zarządzania bezpieczeństwem firmy można się nauczyć?

Wszyscy wiemy, że nie żyjemy w czasach renesansu gdy można było potrafić i znać się na wszystkim. Dzisiaj, w związku z ogromem wiedzy w każdej dziedzinie obowiązuje ścisła specjalizacja i dlatego w odpowiedzialnych firmach, także bezpieczeństwem najczęściej zajmują się specjaliści, zaczynając od **compliance oficerów poprzez audytorów, ochronę, detektywów, ale także specjalistów od spraw kadrowych, bhp, planowania, komunikacji czy informatyki, a także wielu innych dziedzin. I wszyscy oni pracują na to aby firma omijała rafy, które niesie życie.**

Tu jednak warto zwrócić uwagę na to, że nie wystarczy zatrudnić w firmie wszystkich wyżej wymienionych specjalistów, aby powiedzieć, że zrobiliśmy wszystko, aby zapewnić jej bezpieczeństwo. Mało tego, nieraz nie potrzeba (o ile jakieś szczególne przepisy prawne do tego nas nie obligują) tworzyć specjalnych etatów dla zatrudnienia tych wszystkich fachowców. Najważniejsze jest to, aby w firmie była osoba, która potrafi zarządzać bezpieczeństwem, a nie jest to, jak można się domyślać, łatwa sprawa.

Osoba zarządzająca bezpieczeństwem biznesu powinna bowiem, oprócz typowych umiejętności managerskich, posiadać podstawową wiedzę z takich dziedzin jak ekonomia czy prawo oraz znać możliwości, także techniczne, pozwalające na pracę wywiadowczą oraz kontrwywiadowczą.

Oczywiście. takim zarządzaniem bezpieczeństwem może zajmować się sam przedsiębiorca (niestety wielu z poznanych przeze mnie przedsiębiorców myśli, że to robi), ale tak naprawdę nie ma on z reguły wspomnianych wyżej: **wiedzy, umiejętności i doświadczenia.**

Dlatego też najlepszym rozwiązaniem jest, aby przedsiębiorca znał podstawy zarządzania bezpieczeństwem dzięki np. odbyciu choćby studiów podyplomowych w tym zakresie (wystarczy też przejście dobrego i merytorycznego szkolenia), jednak bieżące zajmowanie się tym zagadnieniem przekazał specjaliście, czyli takiemu managerowi bezpieczeństwa biznesu.

KIM JEST BEZPIECZNIK?

Coraz częściej dostrzegam, że przedsiębiorcy korzystają w firmach z usług tzw. bezpieczników, czyli tworzą stanowiska np. oficerów ds. bezpieczeństwa. Popełniają przy tym często dwa podstawowe błędy:

- Zatrudniają na to stanowisko najczęściej **byłych policjantów** lub przekazują te obowiązki **tzw. compliance officerom**, czyli najczęściej, jak pokazuje praktyka, prawnikom – bo przecież oni się na tym znają;
- Uznają, że **wiedza i umiejętności posiadane przez tą osobę są na tyle wystarczające**, że ochronią ich już na zawsze przed nieprzewidzianymi zdarzeniami.

Od razu zaznaczam, że nie mam nic przeciw byłym policjantom zajmującym się bezpieczeństwem biznesu, w końcu sam jestem byłym policjantem. Podobnie, jak nie mam nic przeciw prawnikom. Sam jestem prawnikiem z wykształcenia. Zauważam jedynie, że są policjanci zajmujący się w trakcie służby np. ruchem drogowym czy prewencją i oni niekoniecznie znają się na aspektach koniecznych, aby prawidłowo zajmować się sprawami związanymi z wywiadem czy kontrwywiadem ekonomicznym, pozyskiwaniem informacji potrzebnych do przewidywania potencjalnych zagrożeń.

Podobnie jak policjanci z pionu kryminalnego nie zawsze są przygotowani do prawidłowego zorganizowania ochrony firmy. To samo dotyczy prawników, skupionych na co dzień np. na przygotowywaniu umów handlowych.

Co do drugiego błędu, chodzi o lekceważący stosunek do bieżącej edukacji osób zajmujących się bezpieczeństwem w organizacji.

PODSUMOWANIE

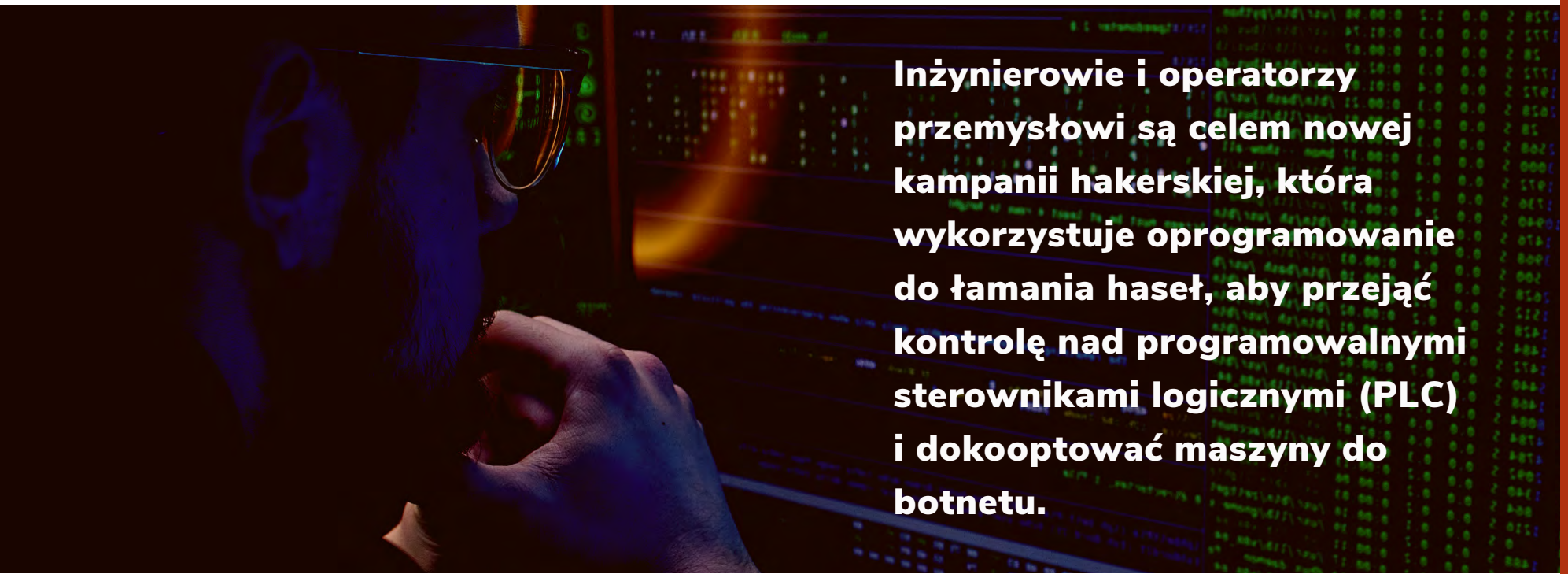
Podsumowując uważam, że w dobie ciągłych i wciąż nowych zagrożeń dla prowadzonych biznesów, bardzo wskazane jest aby przedsiębiorca zdobył wiedzę o podstawowych elementach zarządzania kryzysowego oraz wymuszał na osobach, którym powierza bezpieczeństwo swojego biznesu ciągłe doskonalenie swojej wiedzy i umiejętności.

Warto też pamiętać, że lekceważenie kwestii zarządzania ciągłością działania może skutkować nie tylko stratami finansowymi czy wizerunkowymi ale niejednokrotnie kończy się kłopotami karnymi.


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

HAKERZY ROZPOWSZECHNIAJĄ NARZĘDZIE DO ŁAMANIA HASEŁ

Redakcja
SECURITY MAGAZINE



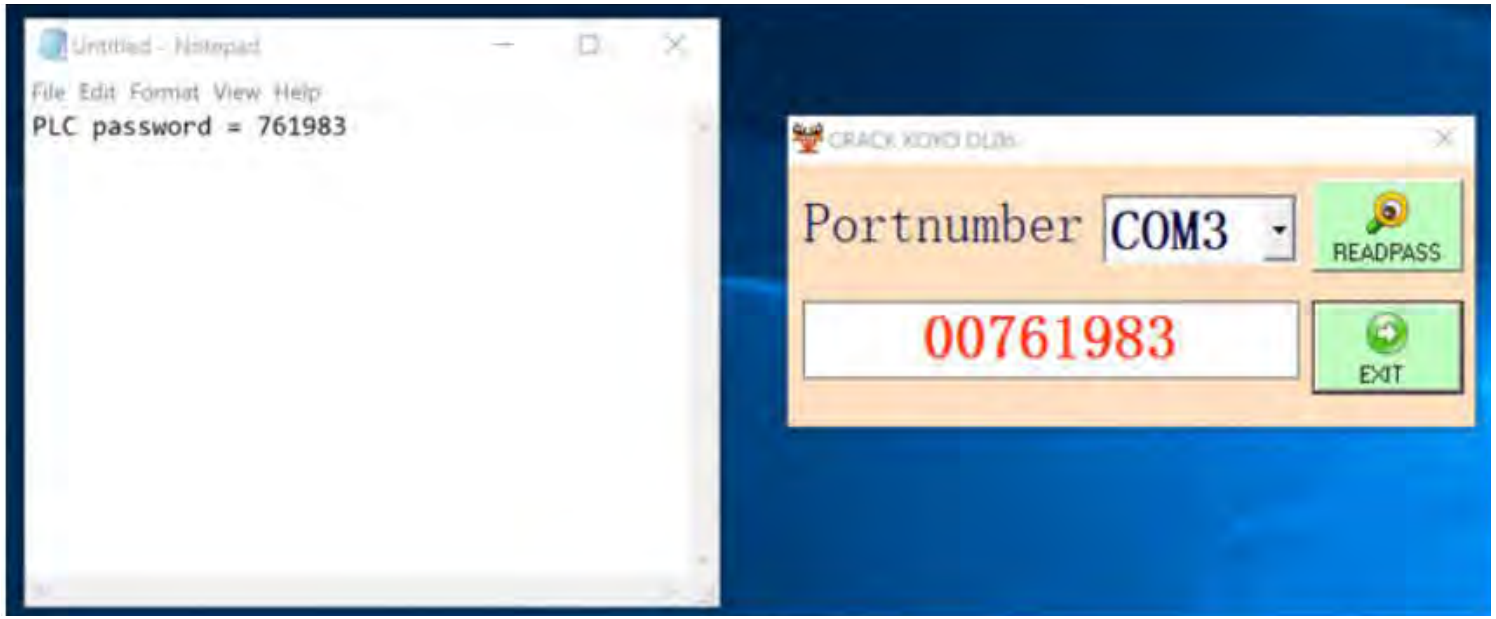
Inżynierowie i operatorzy przemysłowi są celem nowej kampanii hakerskiej, która wykorzystuje oprogramowanie do łamania haseł, aby przejąć kontrolę nad programowalnymi sterownikami logicznymi (PLC) i dokooptować maszyny do botnetu.

- *Oprogramowanie wykorzystywało lukę w oprogramowaniu, która pozwalała na odzyskanie hasła na polecenie* – powiedział **badacz bezpieczeństwa, Dragos Sam Hanson**, dodając: - *Co więcej, oprogramowanie było dropperem złośliwego oprogramowania, infekującym komputer złośliwym oprogramowaniem Sality i przekształcającym hosta w peera w botnecie peer-to-peer Sality.*

[od red.: Sality to klasyfikacja rodziny złośliwego oprogramowania (malware), które infekuje pliki w systemach Microsoft Windows.]

Firma zajmująca się cyberbezpieczeństwem przemysłowym stwierdziła, że exploit odzyskiwania hasła osadzony w dropperze szkodliwego oprogramowania ma na celu odzyskanie poświadczeń związanych ze sterownikiem Automation Direct DirectLOGIC 06 PLC .

Exploit, oznaczony jako CVE-2022-2003 (wynik CVSS: 7,7), został opisany jako przypadek przesyłania poufnych danych w postaci zwykłego tekstu, który może prowadzić do ujawnienia informacji i nieautoryzowanych zmian. Problem został rozwiązany w oprogramowaniu układowym w wersji 2.72 wydanej dwa miesiące temu.



Punktem kulminacyjnym infekcji jest wdrożenie złośliwego oprogramowania Sality do wykonywania zadań, takich jak wydobywanie kryptowalut i łamanie haseł w sposób rozproszony, a także podejmowanie kroków, aby pozostać niewykrytym przez zamknięcie oprogramowania zabezpieczającego działającego na zaatakowanych stacjach roboczych.

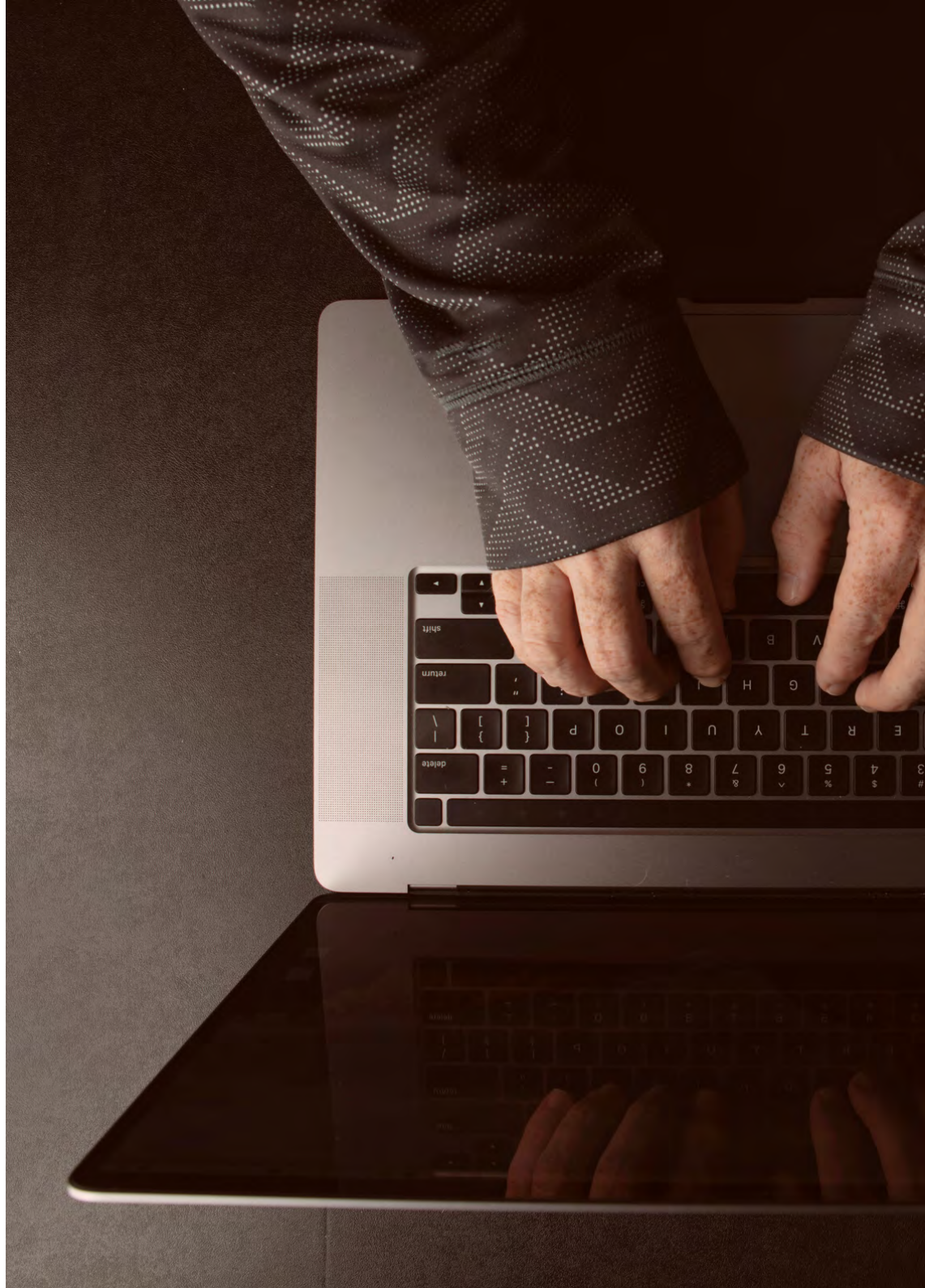
Co więcej, artefakt wydobyty przez Dragosa upuszcza ładunek krypto-clippera, który kradnie kryptowalutę podczas transakcji, zastępując oryginalny adres portfela zapisany w schowku adresem portfela atakującego.

Automation Direct nie jest jedynym dostawcą, na który ma to wpływ, ponieważ narzędzia twierdzą, że obejmują kilka sterowników PLC, interfejsy człowiek-maszyna (HMI) i pliki projektów obejmujące Omron, Siemens, ABB Codesys, Delta Automation, Fuji Electric, Mitsubishi Electric, Proface Schneider Electric, Vigor PLC, Weintek, Allen-Bradley z Rockwell Automation, Panasonic, Fatek, IDEC Corporation i LG.

- Ogólnie rzecz biorąc, wygląda na to, że istnieje ekosystem dla tego typu oprogramowania – zauważył Hanson, przypisując ataki przeciwnikowi o prawdopodobnie motywacji finansowej. - Istnieje kilka stron internetowych i wiele kont w mediach społecznościowych, które promują „łamacze haseł” - dodał.

Nie jest to pierwszy przypadek, w którym strojanizowane oprogramowanie wyodrębniło sieci technologii operacyjnej (OT). W październiku 2021 roku Mandiant ujawnił, w jaki sposób legalne, przenośne, wykonywalne pliki binarne są zagrożone przez różne złośliwe oprogramowanie, takie jak m.in. Sality, Virut i Ramnit.

Na podstawie: **Hackers Distributing Password Cracking Tool for PLCs and HMIs to Target Industrial Systems,** *Ravie Lakshmanan, publikacja 18.07.2022, The Hacker News,* **Screen:** *Hackers Distributing Password Cracking Tool for PLCs and HMIs to Target Industrial Systems, Ravie Lakshmanan.*



ZOSTAŃ EKSPERTEM

SECURITY MAGAZINE

PROMUJ SWOJĄ MARKĘ! BUDUJ WIZERUNEK SWOJEJ FIRMY LUB SIEBIE SAMEGO, SIEBIE SAMEJ

REDAKCJA@SECURITYMAGAZINE.PL

EKSPERCI WYDANIA

DARIUSZ POLACZYK
Risk&Security Manager
Currency One SA.

INSP. DR MARIUSZ CIARKA
Rzecznik Prasowy
Komenda Główna Policji

CHRISTIAN PUTZ
Country Manager
Vectra AI

MACIEJ MISACZEK
Product Manager
systemu impero 360
UNICARD SA

Kierował komórkami zarządzania ryzykiem operacyjnym oraz przeciwdziałania przestępstwom w sektorze bankowym. Pełnił aktywną rolę w Związku Banków Polskich. W latach 2005-2017 w Prezydium Rady Bezpieczeństwa Banków Związku Banków Polskich, przez 10 lat pełnił funkcję Przewodniczącego. Wykładowca Wyższej Szkoły Policji w Szczytnie, Szkoły Policji w Pile oraz Akademii Leona Koźmińskiego w Warszawie.

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.

Odpowiada za działania firmy w Austrii i Europie Środkowo-Wschodniej. Jego rolą jest wspieranie ekspansji firmy w tym rejonie i rozwijanie jej rynkowej strategii. Od wielu lat pełni kluczowe funkcje wykonawcze w wiodących firmach z branży IT, odpowiadając za działy sprzedaży, rozwoju biznesu czy operacji biznesowych.

Specjalizuje się w rozwiązaniach dedykowanych kontroli dostępu. Jest odpowiedzialny za chmurowy system KD – impero 360, a także za monitorowanie trendów Access Control as a Service (ACaaS) i rozwijanie aplikacji.

EKSPERCI WYDANIA

BARTOSZ ADAMCZAK
Account Manager
Marken
dystrybutor Bitdefender w Polsce

Związany z branżą PR od prawie 5 lat. Interesuje się tematyką antywirusów oraz nowinek z tym tematem związanych. Hobbystycznie analizuje i porównuje licencje wiodących marek antywirusów. Również tworzy materiały prasowe o cyberbezpieczeństwie.

TOBIASZ BĄKOWSKI
Kierownik Działu Marketingu
C&C Partners

Od początku pracy w firmie C&C Partners związany z systemami bezpieczeństwa. Pracę zaczynał jako osoba wdrażająca systemy, następnie pracował na stanowisku kierownika ds. serwisu, a w latach 2018 - 2021 pełnił funkcję kierownika ds. produktu. Obecnie kieruje działem marketingu. Zdobytą wiedzą i doświadczeniem chętnie dzieli się z innymi.

JAKUB JACEK
Owner & founder
jakubjacek.pro

Prowadzi Agencję Reklamową zajmującą się realizacją kampanii reklamowych online, które sprzedają. Razem z zespołem projektuje, testuje, wdraża i optymalizuje – wszystko w oparciu o twarde dane i jasne wyniki.

DARIA SADOWSKA
CMO
Firmao

Specjalistka ds. marketingu, zarządzania, PR i HR. W Firmao może realizować się w każdej uwielbianej przez siebie dziedzinie i wymyślać nowe strategie rozwoju. Na co dzień miłośniczka książek współpracująca z ponad 20 wydawnictwami oraz markami na Instagramie. Kobieta zarażająca pozytywnym podejściem do życia.

EKSPERCI WYDANIA

MACIEJ ZYGMUNT
Właściciel
Agencja Bezpieczeństwa
i Detektywistyki

Współzałożyciel Stowarzyszenia Praktycy Compliance, właściciel Agencji Bezpieczeństwa i Detektywistyki, były Naczelnik Wydziału CBŚ, detektyw, wykładowca na Wyższej Szkole Bankowej, Wyższej Szkole Bezpieczeństwa oraz Wyższej Szkole Gospodarki Euroregionalnej.

MICHAŁ ŁĘCKI
Key Account Manager Moxa
Elmark Automatyka

Specjalista ds. cyberbezpieczeństwa, prelegent najważniejszych konferencji poświęconych temu zagadnieniu oraz pomysłodawca i współautor tegorocznego Raportu Cyberbezpieczeństwa OT.

PARTNERZY WYDANIA

KOMENDA GŁÓWNA POLICJI

VECTRA AI

FIRMA ZAJMUJĄCA SIĘ
CYBERBEZPIECZEŃSTWEM
Z SIEDZIBĄ W KALIFORNII

POLITYKA BEZPIECZEŃSTWA

SERWIS INFORMACJNY
O BEZPIECZEŃSTWIE FIRM

RZETELNY REGULAMIN

BLOG POŚWIĘCONY
POLSKIEMU E-COMMERCE

POLICJA

VECTRA®

Polityka® Bezpieczeństwa

Rzetelny® Regulamin

ZOBACZ WYDANIA

Wydanie 1/2022

POBIERZ

Wydanie 2/2022

POBIERZ

Wydanie 3/2022

POBIERZ

Wydanie 4/2022

POBIERZ

Wydanie 5/2022

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