05/2022

SECURITY MAGAZINE

Bezpieczeństwo | Technologia | Wiedza | Najlepsze standardy

Polisa cyber zapewni Ci bezpieczeństwo w sieci

Zasilacze awaryjne UPS w firmach

Cyberbezpieczeństwo instytucji finansowych w świetle regulacji DORA

Czy branża PR jest odporna na cyberataki? Wywiad

Bezpieczeństwo routerów firmowych

SPIS TREŚCI

Rozstrzygnięcie konkursu "Eksperci Security Magazine" 4

W jaki sposób polisa cyber może zapewnić bezpieczeństwo w sieci? 5

PATRONAT: Cyberbezpieczeństwo i technologie na Kongresie PR 13

Czy branża PR jest odporna na cyberataki? Wywiad 15

25 proc. Polaków chce pracować w IT, 33 proc. już szkoli się w tym kierunku 22

Zasilacze awaryjne UPS w firmach 28

Cyberbezpieczeństwo instytucji finansowych w świetle regulacji DORA 34

Chcesz korzystać z Face recognition? Oto warunki, na jakich możesz to zrobić 42

Znaczenie wyroku Schrems II dla transferu danych osobowych 53

Edukacja kluczem do poprawy cyberbezpieczeństwa w firmie 60

Bezpieczeństwo routerów firmowych 67

Czy w aptekach będzie bezpieczniej? 75

SZANOWNI PAŃSTWO,

niezmiernie cieszy nas, że bezpieczeństwo w firmach, a dokładniej cyberbezpieczeństwo coraz częściej staje się tematem publicznych debat, kongresów, spotkań. Obserwujemy coraz większe zainteresowanie szkoleniami, webinarami związanymi właśnie z security.

Mało tego, coraz więcej badań poświęconych jest cyberbezpieczeństwu w biznesie, jak chociażby to realizowane obecnie przez Instytut Rozwoju Społeczeństwa Informacyjnego. Fundacja realizuje pierwszy w Polsce projekt dotyczący branży public relations. Na łamach "Security Magazine" znajdziecie Państwo wywiad z organizatorem badania, zachęcam gorąco do lektury.

Miło nam również poinformować, że już 15-16 września odbędzie się kolejna edycja Kongresu Profesjonalistów PR, którego tematem przewodnim będzie także cyberbezpieczeństwo, a "Security Magazine objęło patronat medialny nad tym wydarzeniem.

Zapraszam do lektury.

Rafał Stępniewski

Rozstrzygnięcie konkursu EKSPERCI SECURITY MAGAZINE

Dla tych, którzy chcą **dotrzeć do tysięcy potencjalnych klientów czy partnerów biznesowych** lub myślą o budowaniu pozytywnego wizerunku swojej firmy w **branży security,** razem z "Nowym Marketingiem" przygotowaliśmy konkurs.

Firmy, które wzięły w nim udział, otrzymały szansę promocji bez angażowania środków finansowych. Nagrodami wartymi kilka tysięcy złotych są nie tylko publikacje eksperckie, ale także pokazanie potencjału firmy, bezpłatne reklamy i wizytówki ekspertów oraz firmowe. Konkurs polegał na zaproponowaniu ciekawego tematu, o którym jego uczestnik chciałby napisać artykuł na łamach naszego e-pisma.

Konkurs skierowany był do czytelników "Nowego Marketingu" i okazało się, że zainteresowanie przerosło nasze oczekiwania. Aż 360 ekspertów odpowiedziało na naszą akcję skierowaną do firm zajmujących się szeroko rozumianym bezpieczeństwem w biznesie.

Wobec ogromnego odzewu redakcja "Security Magazine" zdecydowała, by II i III miejsce przyznać ex aequo.

Oto zwycięzcy:

I miejsce: **Currency One**

II miejsce: **Davidson Consulting oraz Seris Konsalnet**

III miejsce: **Firmao oraz Kancelaria Radcy Prawnego Artur Woźniak**

Gratulujemy!

Redakcja "Security Magazine"

ZAPISZ SIĘ

NA

NEWSLETTER

BY NIE PRZEOCZYĆ

KOLEJNEGO WYDANIA

SECURITY MAGAZINE

W JAKI SPOSÓB POLISA CYBER MOŻE ZAPEWNIĆ BEZPIECZEŃSTWO W SIECI?

Piotr Cholewczyński
Infinity Brokerzy Ubezpieczeniowi Sp. z o.o.

Nikogo już nie dziwią pojawiające się codziennie doniesienia o coraz to nowych atakach hackerskich. Niemniej cały czas funkcjonuje przeświadczenie, że „ten problem mnie nie dotyczy". Statystyki, do których mamy praktycznie nieograniczony dostęp, pokazują jednak, że liczba ataków hackerskich w Polsce w ostatnich dwóch latach rośnie wręcz lawinowo i w zasadzie nikt nie powinien czuć się bezpieczny.

Obecna sytuacja geopolityczna, w tym tocząca się wojna rosyjsko–ukraińska, dodatkowo intensyfikują liczbę incydentów cybernetycznych. Coraz więcej ukraińskich spółek próbuje przenieść swoją działalność do Polski. Okazuje się, że na terenie naszego kraju padają one bardzo często ofiarą ataków rosyjskich hackerów lub osób działających na zlecenie Rosji, co odbija się niejako rykoszetem również na polskich firmach.

NARZĘDZIA DO WALKI Z HACKERAMI

Poza narzędziami w ramach software/hardware oraz procedurami ograniczania dostępów, które mają na celu minimalizację wystąpienia ataków, istnieje możliwość przeniesienia części ryzyka związanego z konsekwencjami ataku hackerskiego **na ubezpieczyciela.**

Dzieje się to poprzez zakupienie odpowiedniego ubezpieczenia od ryzyk cybernetycznych.

Ubezpieczenie od ryzyk cybernetycznych - zwane potocznie Cyber - zapewnia ochronę przede wszystkim przed skutkami ataków hackerskich (w tym np. ransomware, czy zwrot kosztów okupu) na infrastrukturę ubezpieczonego, włączając

UBEZPIECZENIE OD RYZYK CYBERNETYCZNYCH ZAPEWNIA OCHRONĘ PRZED SKUTKAMI ATAKÓW HACKERSKICH (NP. RANSOMWARE, ZWROT KOSZTÓW OKUPU) NA INFRASTRUKTURĘ UBEZPIECZONEGO.

w to również utracone korzyści i zwiększone koszty prowadzonej działalności. Ubezpieczyciel pokrywa także wydatki związane z wynajęciem informatyków śledczych, prawników oraz podmiotów specjalizujących się w usługach w zakresie zarządzania kryzysowego i public relations. Drugim istotnym elementem ubezpieczenia Cyber jest ochrona w zakresie nałożonych kar administracyjnych.

Ubezpieczyciel zwróci nie tylko wysokość opłaconych kar administracyjnych za naruszenie przepisów o ochronie danych osobowych (w tym m.in. RODO), ale również pokryje koszty, które wynikają z obowiązku zgłoszenia takiego incydentu do odpowiednich organów nadzoru i osób, których dane zostały naruszone.

DLA KOGO CYBER?

Dzisiaj każdy podmiot niezależnie od reprezentowanego sektora gospodarki narażony jest na ataki hackerskie więc ubezpieczenie Cyber dedykowane jest dla wszystkich.

Szczególnym przykładem mogą być spółki posiadające własną infrastrukturę on-premise lub infrastrukturę kolokowaną oraz spółki przetwarzające duże ilości danych. Ich wyciek lub naruszenie może powodować bowiem istotne konsekwencje finansowe, prawne i reputacyjne.

Innym przykładem są zakłady produkcyjne tzw. przemysłu 4.0 opierające swoją działalność na zarządzaniu procesem technologicznym za pomocą rozwiązaniach sieciowych, IoT itp.

Cechą wyróżniającą ubezpieczenie Cyber jest możliwość maksymalnego dostosowania zakresu ochrony do rzeczywistych wydatków w przypadku wystąpienia ataku hackerskiego. Ubezpieczenie w szerokim stopniu pokrywa poniesione koszty, które są najczęściej bardzo wysokie i konieczne do zaangażowania w krótkim czasie po ujawnieniu incydentu cybernetycznego.

NA CO JESZCZE MOŻEMY LICZYĆ

Powyższe to już standard, który jest oferowany przez wszystkich ubezpieczycieli w zasadzie „od ręki". W ostatnim czasie można jednak zauważyć, że ubezpieczenia Cyber ewoluują, zmierzając w stronę rozszerzenia o usługi zaliczane do tzw. assistance. Ubezpieczyciele, którzy posiadają bardzo mocno rozwinięte linie produktowe Cyber dodali dwie istotne usługi (SOC i Cyber Response Team) mające na celu aktywną ochronę w zakresie network security dla ubezpieczanych firm.

SOC OD UBEZPIECZYCIELA

Zespoły SOC (Security Operations Center) śledzą każdy niestandardowy ruch na infrastrukturze ubezpieczonego. Dzięki temu klient posiada możliwość bieżącego wglądu, czy jego infrastruktura nie padła ofiarą ataku hackerskiego.

TO NAPRAWDĘ DZIAŁA!

Na początku toczącej się obecnie wojny otrzymaliśmy zgłoszenie od współpracującego z nami zagranicznego ubezpieczyciela, że jego zespół SOC zauważył niestandardowy ruch na infrastrukturze jednego z naszych klientów. Klient nie dostrzegł wcześniej żadnych sygnałów mogących świadczyć o przygotowywanym ataku hackerskim.

Ubezpieczyciel przekazał mu wszelkie szczegóły związane z niepożądanym ruchem sieciowym (wraz z informacją odnośnie strony ataku), wskazując jednocześnie szereg zaleceń, które należy wprowadzić w celu ograniczenia możliwości dalszego rozprzestrzeniania się ataku. Jednym z celów atakujących było prawdopodobnie przejęcie danych osobowych (znaczna część zespołu naszego klienta to pracownicy z Ukrainy). Dzięki bardzo szybkiej reakcji ubezpieczyciela oraz zastosowaniu jego zaleceń przez klienta atak okazał się nieskuteczny.

CYBER RESPONSE TEAM OD UBEZPIECZYCIELA

Drugą z dodatkowych usług w ramach ubezpieczenia Cyber są tzw. zespoły reakcji na zdarzenie "Cyber Response Team" działające na zlecenie ubezpieczycieli 24 godziny na dobę 365 dni w roku. Pomagają one ograniczać skutki incydentów cybernetycznych poprzez niezwłoczne wykorzystanie kosztów reakcji na zdarzenie (jeszcze przed zgłoszeniem szkody). Mowa tutaj o eksperckich spółkach (czasami zewnętrznych) powoływanych w imieniu ubezpieczyciela, wspierających w profesjonalny sposób ubezpieczone firmy.

SKRUPULATNA WERYFIKACJA INFRASTRUKTURY KLIENTA

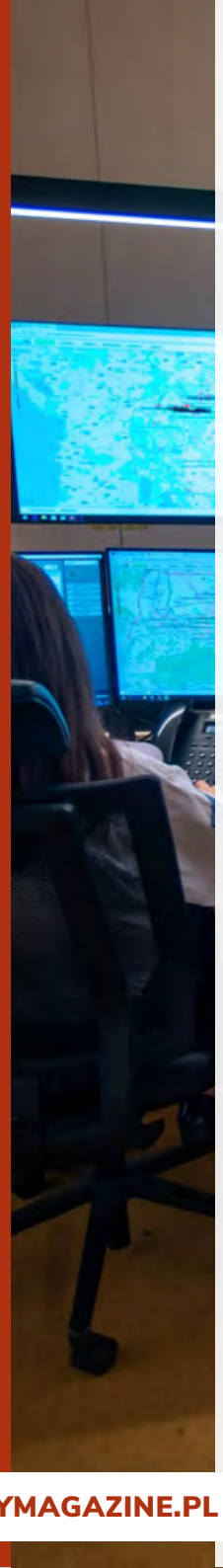
Ubezpieczyciele, którzy wyspecjalizowali się w produkcie Cyber, oferując szeroki pakiet swoich usług chcą mieć pewność, że ryzy-

ODSZKODOWANIE W PRZYPADKU RANSOMWARE

Zostałeś ofiarą ataku ransomware - twoje dane zostały zaszyfrowane? Hackerzy żądają okupu za ich odszyfrowanie?

Ubezpieczyciel wypłaci nie tylko kwotę żądanego okupu, ale zwróci również koszty odtworzenia danych, których nie udało się odszyfrować, pokryje koszty związane z zaangażowaniem specjalistów w zakresie zarządzania kryzysowego, informatyki śledczej, public relations oraz wypłaci odszkodowanie za utracone korzyści, które byłyby możliwe do uzyskania, gdyby nie atak hackerski.

Średnia wysokość okupu w Polsce w związku z atakiem ransomware w ostatnim roku to ponad 600 tys. zł. Sam okup to jednak nie wszystko: wydatki związane z przestojami, utrata zysku, zwiększone koszty prowadzonej działalności, angażowanie informatyków śledczych, zespołów reagowania na incydenty a czasami nawet zespołów specjalizujących się w usługach PR powodują, że przeciętny koszt związany z atakiem ransomware to ponad 7 mln zł.

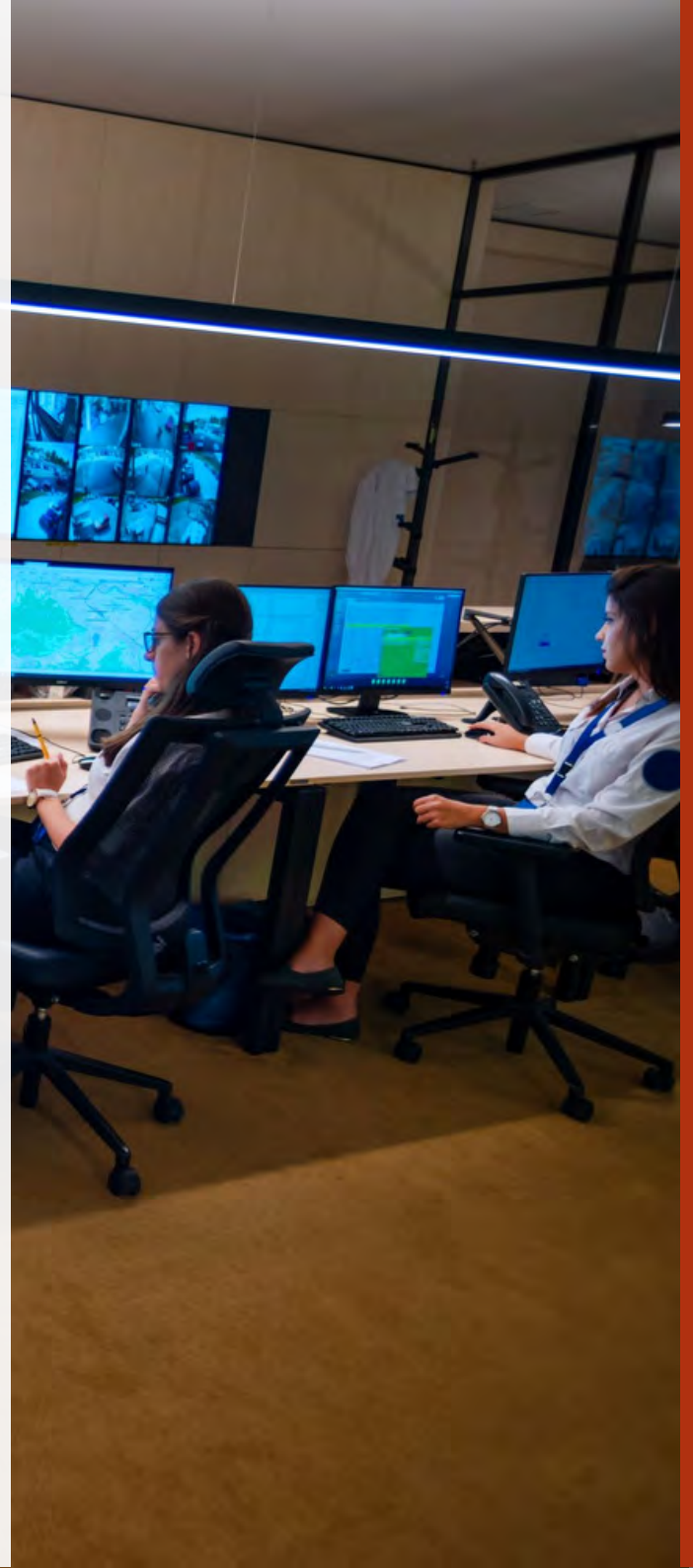


ko, które na siebie przyjmują jest odpowiednie w stosunku do zainkasowanej składki. Nie wystarczy już posiadanie rozbudowanych procedur, systemów zarządzania jakością typu ISO 9001 czy też wieloskładnikowego uwierzytelniania (2FA/MFA) podczas zdalnego łączenia się ze swoimi systemami.

Coraz częściej ubezpieczyciele posiadają narzędzia (w pełni legalne) do weryfikacji infrastruktury potencjalnych klientów, w tym do skanowania ich domen w poszukiwaniu otwartych portów, niewspieranego oprogramowania czy też weryfikacji łatania istotnych podatności CVE. Jest to bardzo korzystne rozwiązanie również dla klienta, ponieważ otrzymuje niejako przy okazji pełny raport na ten temat. Na przykład bardzo często okazuje się, że stare otwarte porty, które ułatwiają przeprowadzenie skutecznego ataku hackerskiego, są pozostałościami po nieaktualnych już projektach i można je niezwłocznie zamknąć.

PODSUMOWANIE

Dynamika, z jaką mamy do czynienia w przypadku ataków hackerskich powoduje, że ubezpieczyciele muszą podążać za potrzebami potencjalnych “ofiar”. Niektórzy z nich zauważyli, że czasami warto wspomóc klienta nie tylko w momencie powstania incydentu, angażowania kosztów reakcji na zdarzenie, ale również na znacznie wcześniejszym etapie - śledząc niepożądany ruch sieciowy przez własne lub outsourcingowane SOC.



W jaki sposób polisa cyber może zapewnić bezpieczeństwo w sieci?

Bardzo podobnie sytuacja wygląda na rynku usług IT, na którym widać coraz większe zapotrzebowanie na specjalistów z zakresu network security. Na skutek obecnej sytuacji związanej z licznymi atakami hackerskimi świat IT i świat ubezpieczeń zbliżyły się do siebie, podejmując wspólne działania utrudniające aktywność cyberprzestępców.

ODSZKODOWANIE ZA NARUSZENIE ZASAD RODO I INNYCH PRZEPISÓW ZWIĄZANYCH Z ZACHOWANIEM POUFNOŚCI DANYCH

W związku z naruszeniem poufności danych osobowych (RODO) nałożono na twoją firmę karę administracyjną. Ubezpieczyciel zwróci nie tylko koszty jej pokrycia, ale również wydatki poniesione na poinformowanie odpowiednich organów oraz osób, których dane zostały naruszone, koszty związane z zatrudnieniem specjalistów w zakresie public relations, koszty prawników, którzy byli zaangażowani w procedurę zgłoszenia naruszenia danych do odpowiednich organów nadzoru oraz osób, których dane zostały naruszone.

Wykaz kar administracyjnych nałożonych przez Urząd Ochrony Danych Osobowych (UODO) znajdziesz na stronie UODO.

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**

Cyberbezpieczeństwo i technologie na Kongresie PR

PATRONAT
SECURITY MAGAZINE

XXII Kongres Profesjonalistów Public Relations, który ściągnie do Rzeszowa ekspertów z branży PR, już 15-16 września. Dwa dni wypełnione będą spotkaniami i rozmowami na temat technologii w komunikowaniu, cyberbezpieczeństwa, a także zmian, jakie dokonują się w narzędziach wykorzystywanych przez specjalistów zajmujących się PR.

W Bristol Tradition & Luxury Hotel inspirować i komentować rzeczywistość będą m.in.:

- Małgorzata Fraser, Dziennikarka CyberDefence24.pl,
- Michał Rosiak, Ekspert i Edukator Cyberbezpieczeństwa, Bloger – CERT Orange Polska,
- Błażej Szymczak, Chief Security Officer w MODIVO S.A.,
- Anna Klimczuk, Dyrektor Komunikacji w polskim oddziale Microsoft,
- Monika Borzdyńska, Członek Zarządu operatora PGE Narodowego,
- Małgorzata Bajer, Dyrektor ds. Komunikacji, Promocji i Marketingu, Rzecznik Prasowy, PGE Narodowy,
- Tomasz Kułakowski, Rzecznik Prasowy Krynica Vitamin, Były Korespondent Polsatu w Moskwie,
- Deniz Rymkiewicz, CEE Communications Manager, Klarna,
- Anna Olszewska, Dyrektor Departamentu Komunikacji, Krajowa Izba Rozliczeniowa S.A.,
- Sebastian Bykowski, Prezes Zarządu, Dyrektor Generalny PRESS-SERVICE Monitoring Mediów,
- Magdalena Grochala, Ekspertka w zakresie komunikacji i public relations,
- Adam Łaszyn, Prezes Zarządu ALERT MEDIA Communications,
- dr hab. Jarosław Flis, Prof. UJ, Socjolog,
- Łukasz Świerżewski, Członek Zarządu Polskiej Agencji Prasowej,
- i wielu innych gości.

SECURITYMAGAZINE.PL

PATRONAT
SECURITY MAGAZINE

Oprócz wystąpień prelegentów, podczas Kongresu zorganizowane zostaną także panele dyskusyjne, w tym jeden poświęcony kwestiom cyberbezpieczeństwa. Jest to jedno z poważniejszych wyzwań stojących obecnie przed praktykami public relations. Zmianom związanym z zabezpieczeniem organizacji towarzyszą również kryzysy, które z niespotykaną dotąd siłą dotykają coraz więcej podmiotów gospodarczych.

- Dziwny czas zagrożenia, jaki wywołała w społeczeństwie pandemia COVID-19, spowodował liczne zmiany zarówno społeczne, jak i ekonomiczne. Inaczej podchodzi się także do kwestii związanych z public relations i z komunikacją. I, gdy już myśleliśmy, że nieco wyhamowująca pandemia pozwoli nam odetchnąć, napaść Rosji na Ukrainę zdestabilizowała względną normalność w każdej dziedzinie życia. Co na to PR? Czas wojny wymaga innego podejścia do działań komunikacyjnych i strategicznego zarządzania. Na co zwrócić uwagę, kto dziś dobrze sobie radzi, a kogo nie warto naśladować? Jakie są w tym wszystkim miejsce i rola nowych technologii? Jak zmieniają one public relations i jak są przez PR wykorzystywane? - mówią organizatorzy Kongresu Profesjonalistów PR.

Kongres odbędzie się w formie hybrydowej. Zgłoszenia uczestnictwa stacjonarnego, jak i online przyjmowane są do 2 września. Zapisu na wydarzenie możesz dokonać TUTAJ.

"Security Magazine" jest patronem medialnym
XXII Kongresu Profesjonalistów PR.

Fot. Kongres Profesjonalistów PR

CZY BRANŻA PR JEST ODPORNA NA CYBERATAKI? WYWIAD

Dariusz Tworzydło
Uniwersytet Warszawski, EXACTO

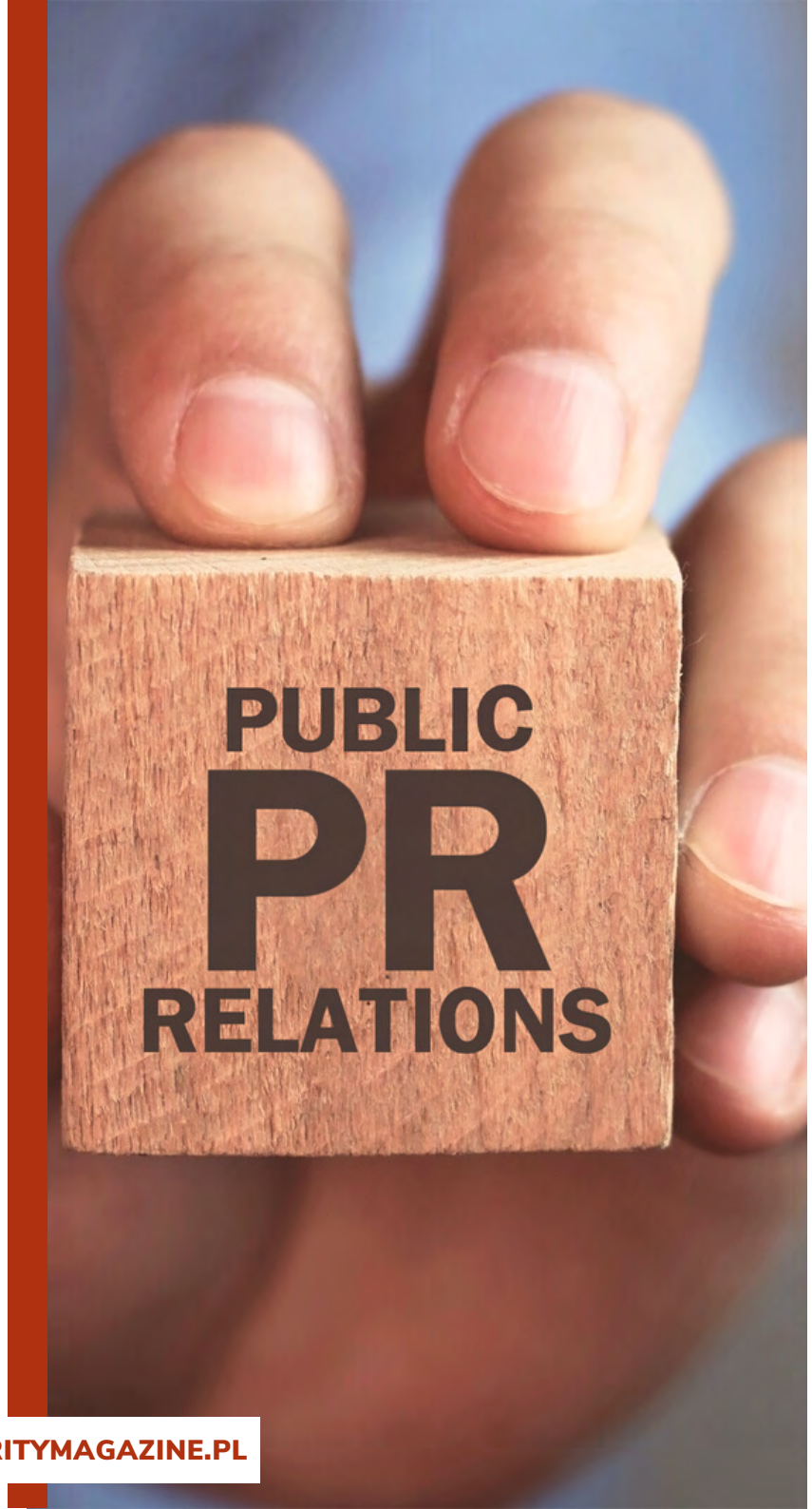
Polska Agencja Prasowa z Instytutem Rozwoju Społeczeństwa Informacyjnego zachęca specjalistów public relations do udziału w ankiecie, badającej po raz pierwszy w Polsce świadomość branży z zakresu cyberbezpieczeństwa, co w dalszej perspektywie ma wpływ na sposób komunikowania i współpracę z klientami. Na pytanie, dlaczego eksperci PR powinni wziąć udział w tym badaniu, odpowiada Dariusz Tworzydło, jeden z czołowych w Polsce ekspertów z zakresu PR.

Od wielu lat m.in. przy wykorzystaniu badań marketingowych niejako włącza Pan branżę PR w istotne z punku widzenia świata czy Polski momenty. Teraz, pod Pana przewodnictwem, trwają badania związane z zagrożeniami, jakie mogą czyhać na PR-owców ze strony cyberprzestępców.

Czy, Pana zdaniem, cyberwojna, która rozpoczęła się końcówką ubiegłego roku, dotyczy też specjalistów od wizerunku?

Nie tylko w Polsce odnotowujemy ostatnio gwałtowny wzrost cyberprzestępstw. Według najnowszego raportu CERT Polska, w 2021 roku obsłużono o 182% więcej incydentów związanych z cyberbezpieczeństwem, niż rok wcześniej. Ta tendencja się nie zatrzyma, bowiem przestępcy poszukują coraz to nowych sposobów na poszerzenie zakresu swoich bezprawnych działań.

Problem pogłębił się jeszcze w wyniku kryzysu na wschodzie. Ochrony przed cyberatakami nie sprowadza się wyłącznie do działań na polu informatyki. Dotyczy to także w szerokim zakresie kwestii komunikowania, zarówno wewnątrz firm czy instytucji, ale także ich współpracy z podmiotami zewnętrznymi. Konieczne jest zabezpieczenie, edukowanie pracowników i kontrahentów oraz informowanie o zagrożeniach.



Jaki jest cel prowadzonego badania?

Badanie jest prowadzone dwutorowo. Skupiliśmy się na dziennikarzach i specjalistach branży PR jako grupach z założenia narażonych na obcowanie z fake newsami, dezinformacją i na cyberataki. Badamy, jak oni postrzegają te problemy. Opinie osób pracujących w mediach i zajmujących się profesjonalnie komunikowaniem, mogą, moim zdaniem, mieć istotne przełożenie na dobre praktyki w analizowanych przez nas obszarach, ale też szersze przełożenie na zachowania społeczne. Mamy taką nadzieję.

Jedno z pytań ankiety skierowanej do PR-owców, wymienia 13 branż, w tym public relations. Respondent musi je pogrupować od 1 do 13 pod względem największego zagrożenia cyberatakami.
A jakie jest Pana zdanie w tej kwestii. Jak bardzo branża może być narażona na działania hakerskie? Czy jest cennym “kąskiem” dla cyberprzestępców, w Pana opinii?

Tak. Wynika to z faktu, że agencje i eksperci public relations często mają dostęp do poufnych informacji, zwią-

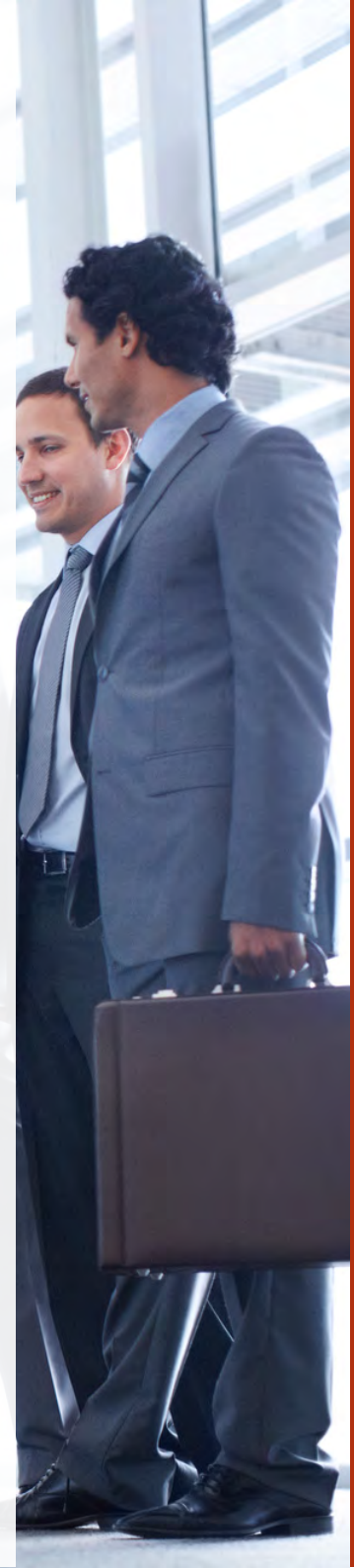
zanych chociażby z komunikowaniem kolejnych decyzji biznesowych firm i instytucji. Wyciek takich danych może zaszkodzić ich klientom, a także im samym. Dlatego właśnie tak ważna jest świadomość tego, jak chronić siebie i swoje dane przed atakami w sieci. Agencje i specjaliści PR muszą także być w awangardzie, jeśli chodzi o świadomość zabezpieczeń i edukowanie.

Wiadomym jest, że najsłabszym ogniwem, jeśli chodzi o ataki hakerskie, jest człowiek. Łatwo go zmanipulować, wyciągnąć poufne dane. Czy agencje PR mogą być dla klientów realnym zagrożeniem?

To prawda, że człowiek często jest najsłabszym ogniwem, jeśli mówimy o bezpieczeństwie i procedurach zabezpieczeń. Taki wyciek danych, gdyby do niego doszło, może mieć poważne konsekwencje wizerunkowe dla samej agencji lub eksperta. Dlatego edukowanie i świadomość zagrożeń są tak ważne. Również transfer dobrych praktyk stosowanych przez te podmioty, zarówno wewnętrznie jak i we współpracy z klientami, podnosi poziom bezpieczeństwa.

Jaka, Pana zdaniem, jest świadomość cyberzagrożeń w branży PR? Wydawałoby się, że ze względu na wiedzę PR-owców dotyczącą m.in. kryzysów wizerunkowych, jest im łatwiej dostrzegać zagrożenia, przewidywać i przeciwdziałać im lub je łagodzić. Czy tak jest również w kontekście cyberbezpieczeństwa?

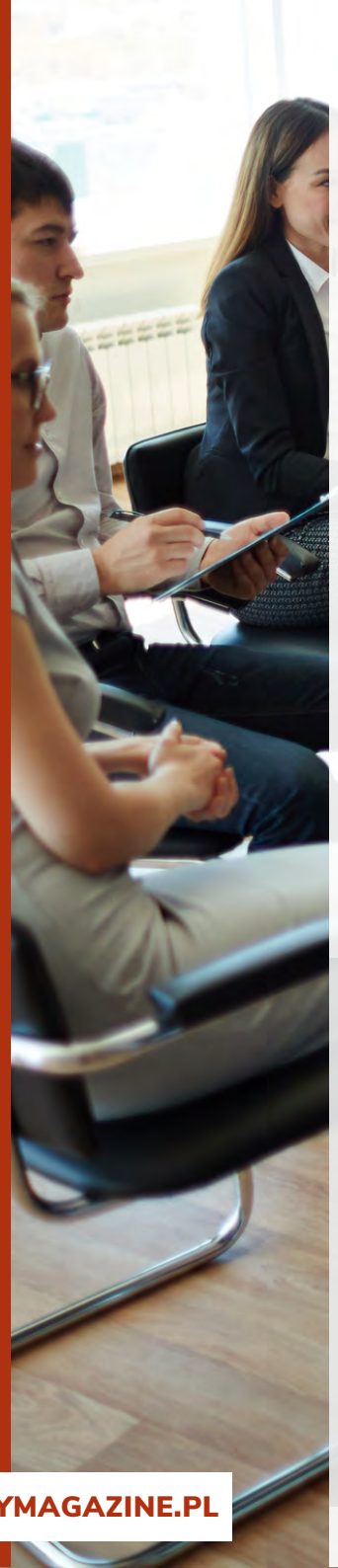
Skalę tego, o co Pani pyta, pokażą na pewno badania. Liczymy na to, że wyniki, zaprezentowane w naszym raporcie i podczas Kongresu Public Relations we wrześniu, wpłyną dodatkowo na zwiększenie zaufania klientów do agencji.



Albo odwrotnie... zaufanie spadnie. A może będzie to asumpt do rewizji stosowanych praktyk. Jeszcze trudno oceniać, ponieważ badanie jest w toku, a z doświadczenia wiem, że wyniki badań mogą zaskoczyć.

Czy agencje PR szkolą się z zakresu cyberbezpieczeństwa?

Branża PR dostrzega znaczenie zagadnień związanych z bezpieczeństwem w sieci. Już we wrześniu w Rzeszowie odbędzie się XXII Kongres Public Relations. Temat przewodni w tym roku brzmi: "Technologie w komunikowaniu. Dezinformacja i cyberbezpieczeństwo." Nasi prelegenci będą rozmawiać m.in. o cyberbezpieczeństwie jako wyzwaniu dla procesów komunikacyjnych, czy o unikaniu pułapek, jakie zastawiają na nas cyberprzestępcy. Specjaliści PR rozumieją, jak ważny jest to problem, dlatego tegoroczny Kongres już teraz cieszy się bardzo dużym zainteresowaniem. Co ciekawe, sam temat został wskazany już podczas zeszłorocznej edycji wydarzenia, co sugeruje, że eksperci przewidywali wzrost znaczenia tego tematu.

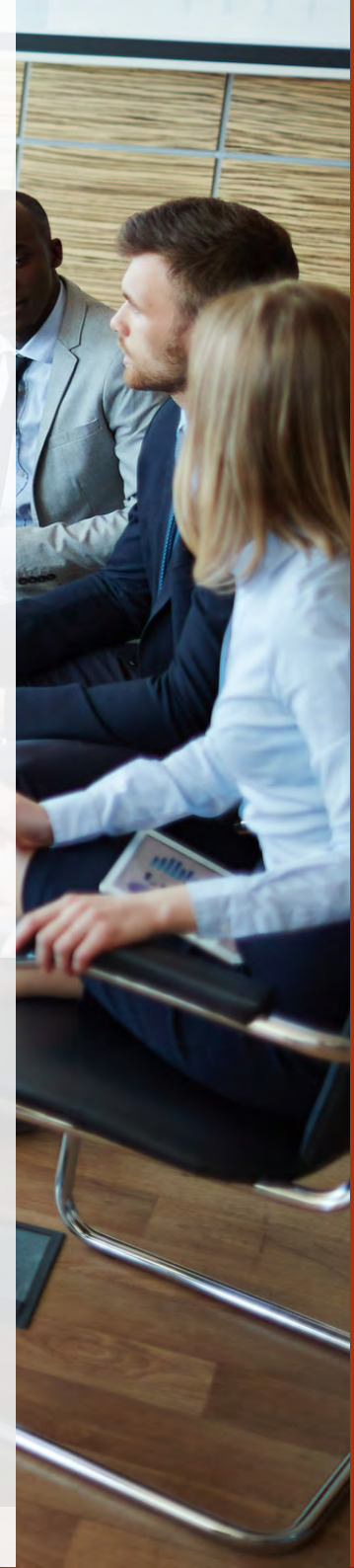


Kiedy możemy spodziewać się wyników ankiety? Gdzie będzie można się z nimi zapoznać?

Wyniki zostaną zaprezentowane właśnie w trakcie Kongresu. Odbędzie się on 15 i 16 września w Rzeszowie. Jestem przekonany, że będą one interesujące dla wszystkich osób, które na co dzień mają do czynienia z tematem bezpieczeństwa w sieci.

Dziękuję za rozmowę.

Rozmawiała: Monika Świetlińska



Chcesz wziąć udział w ankiecie?

Twoje odpowiedzi na pytania w niej zawarte pozwolą na stworzenie mapy zagrożeń pracy specjalisty ds. PR w cyberprzestrzeni.

ANKIETA

OBSŁUGA PRAWNA E-COMMERCE

WWW.RZETELNYREGULAMIN.PL

25 PROC. POLAKÓW CHCE PRACOWAĆ W IT, 33 PROC. JUŻ SZKOLI SIĘ W TYM KIERUNKU

Jacek Mrzygłód
Evolution Poland

Polacy cały czas mocno interesują się branżą IT, co widać w ostatnim raporcie Evolution. Już 24 proc., czyli prawie co czwarty Polak, zastanawia się nad tym, czy przejść do branży IT. Blisko połowa z nas (44 proc.) myśli o tym, ale jest jeszcze niezdecydowana, a 32 proc. z pewnością nie ma takich planów.

– Branża IT cieszy się dużym zainteresowaniem kandydatów, ponieważ w naszej ocenie ma bardzo dużo do zaoferowania. Jak wynika z naszych raportów, pracownicy chwalą pracodawców za dobre i elastyczne warunki pracy. W Evolution bardzo mocno stawiamy na te aspekty i wiemy, że owocowe czwartki to za mało, by odpowiednio docenić pracownika. Branża IT wyznacza standardy w zatrudnieniu oraz relacji pracodawca-pracownik i być może właśnie dlatego aż ¼ Polaków zastanawia się nad przebranżowieniem do tego sektora – komentuje **Konrad Bromiński, Senior HR Manager w Evolution.**

KUSZĄ WYSOKIE ZAROBKI I MOŻLIWOŚĆ ROZWOJU

Twórcy raportu zastanawiali się również nad tym, dlaczego Polacy chcą pracować w IT, co taka praca mogłaby im dać. Jak się okazuje najbardziej kuszą wysokie zarobki, takiej odpowiedzi udzieliło aż 79 proc. badanych. Kolejne aspekty, które są dla nas ważne to możliwość pracy zdalnej (64 proc.) oraz możliwość ciągłego rozwoju (60 proc.). Inne pozytywne strony pracy w IT to: ciekawe projekty (58 proc.), możliwość obcowania z nowymi technologiami (54 proc.), elastyczne podejście do pracownika (44 proc.) oraz work-life-balance (24 proc.).

– W Polsce w roku 2021 działało ponad 91 tys. firm IT związanych z oprogramowaniem. Co ciekawe, ich odsetek, w porównaniu do roku 2020, zwiększył się aż o 20 proc. A tylko w pierwszym kwartale tego roku przybyło ich już ponad 5 proc. Liczby te mogą wynikać nie tylko z rosnącego zapotrzebowania na inżynierów oprogramowania, ale także świadczyć o tym, że polscy programiści często świadczą usługi również dla zagranicznych podmiotów. Nie ma się czemu dziwić – są dobrze wykształceni i zaangażowani w projekty, więc chętnie ich one zatrudniają – mówi **Konrad Bromiński, Senior HR Manager w Evolution.**

To, co skłania Polaków do podjęcia pracy w IT to jedno, firma Evolution idąc tym tropem, zadała również pytanie o to, czego potencjalni kandydaci oczekiwaliby od przyszłych pracodawców w branży. To dobra wskazówka dla osób szukających specjalistów w tym obszarze. Jak się okazuje ankietowani przede wszystkim liczą na atrakcyjne wynagrodzenie (81 proc.), dobrą atmosferę w zespole (65 proc.) i elastyczny czas pracy (60 proc.). Poza tymi trzema czynnikami w zestawieniu znalazła się jeszcze: możliwość pracy z dowolnego miejsca na Ziemi (59 proc.), interesujące projekty (51 proc.), możliwość rozwoju kompetencji (50 proc.) i możliwość awansu (47 proc.).

ZACZYNAJĄC W IT, MOŻNA LICZYĆ NA WSPARCIE BARDZIEJ DOŚWIADCZONYCH

Maja Misiewicz skończyła geodezję na Wojskowej Akademii Technicznej. Zaraz po studiach dostała pracę w Starostwie Powiatowym w Piasecznie w Wydziale Geodezji. Choć szybko udało się jej znaleźć pracę w zawodzie, czuła, że nie jest to zajęcie dla niej.

Jeszcze w czasie studiów interesowała się branżą IT i m.in. skończyła bootcamp backend Dev, językiem wiodącym podczas tego szkolenia była Java, ale były też inne języki i technologie. Kiedy pracowała już w urzędzie, postanowiła rozejrzeć się na rynku pracy. Jej dzisiejsze stanowisko to Junior Data Scientist. Pracuje przy budowie modeli do detekcji obiektów. Jest odpowiedzialna za przygotowanie oraz kontrolę danych, uruchomienie procesu i ocenę osiąganych wyników.

– *Jestem bardzo zadowolona z obecnej pracy. Cieszę się, że podjęłam decyzję przejścia do branży IT przede wszystkim dlatego, że mam możliwość ciągłego uczenia się i podnoszenia swoich kwalifikacji. Miałam też to szczęście, że trafiłam na zespół, który chętnie dzieli się swoim doświadczeniem, podpowiada, gdy przychodzą trudne momenty i wskazuje możliwości rozwoju. Początkowo byłam zagubiona. Dziś sama wprowadzam w tajniki naszej pracy nowych stażystów. Jeśli komuś chodzi po głowie przebranżowienie się do IT, polecam spróbować. W przyszłości myślę o studiach podyplomowych ukierunkowanych na IT, poza tym staram się korzystać ze szkoleń udostępnianych na portalach typu coursera* – komentuje **Maja Misiewicz.**

Osoby, które przechodzą do IT, na początku swojej kariery liczą na wsparcie zespołu, do którego trafią. Część firm w tej branży ma w zwyczaju przyznawać do nowych pracowników mentorów, osoby z doświadczeniem, które poprowadzą nowego pracownika w jego rozwoju. Takie podejście i praca zespołowa pozwala na zdobywanie unikalnych kompetencji w swojej dziedzinie, zwłaszcza, jeśli mowa o firmie, w której wykorzystywane są innowacyjne technologie i rozwiązania.

I rzeczywiście, 23 proc. ankietowanych przyznało, że w przeszłości miało w swojej pracy przydzielonego mentora. Natomiast 17 proc. badanych powiedziało, że nie miało takiej osoby w swojej pracy, ale chciałoby mieć. Zaledwie 3 proc. Polaków stwierdziło, że owszem korzystało ze wsparcia mentora, ale w przyszłości nie chciałoby mieć takiej osoby – co pokazuje, że zdecydowanie większa liczba osób pozytywnie ocenia takie wsparcie.

25 proc. Polaków chce pracować w IT,
33 proc. już szkoli się w tym kierunku

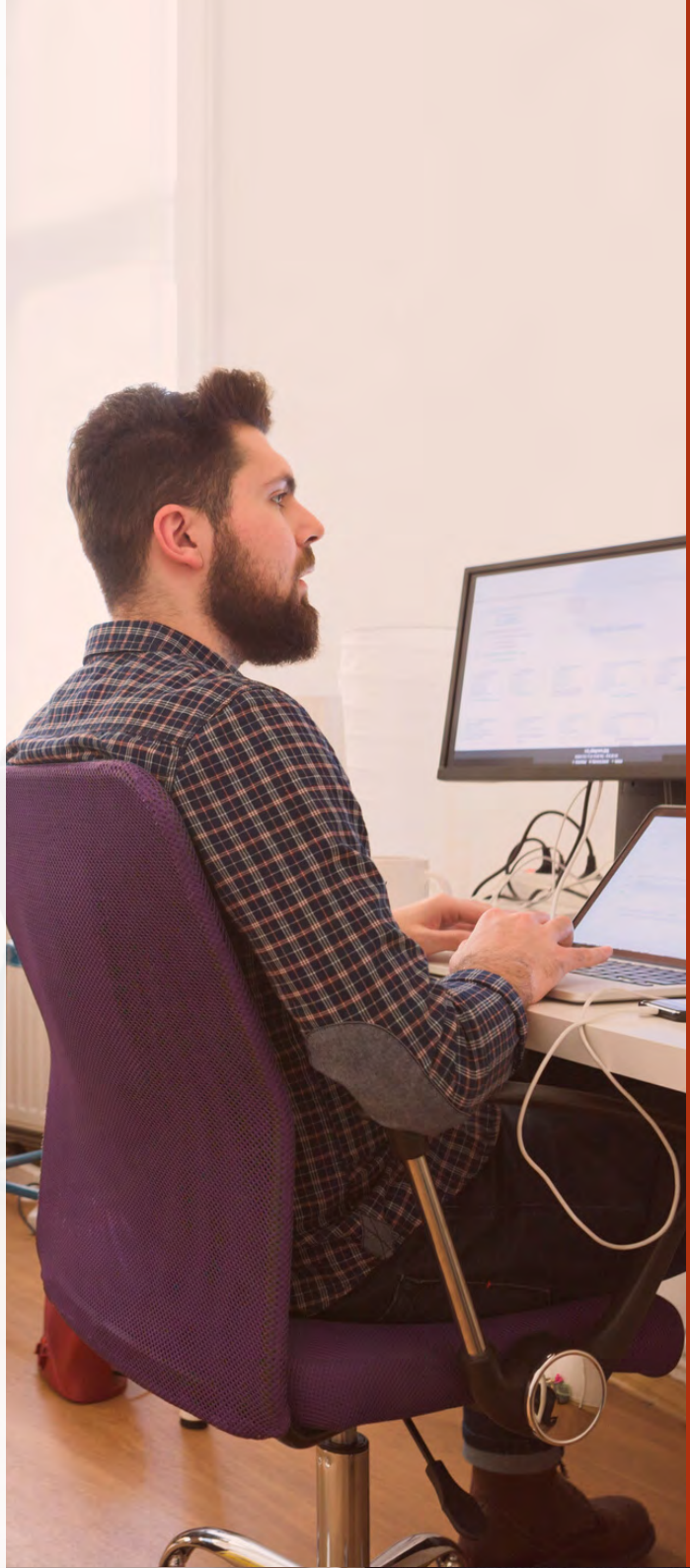
TESTOWANIE OPROGRAMOWANIA I PROGRAMOWANIE NAJCIEKAWSZYMI SPECJALIZACJAMI

Najpopularniejszą specjalizacją, nad którą Polacy zastanawiają się najczęściej, okazało się **testowanie oprogramowania**. Ten obszar wskazało ponad 30 proc. ankietowanych. Kolejną pozycję zajęło programowanie (19 proc.), a zaraz za nim obsługa IT (11 proc.) i analiza danych (11 proc.). Dla 10 proc. Polaków nie ma znaczenia, do jakiej specjalizacji mieliby trafić, przechodząc do IT. Natomiast na samym końcu znalazło się badanie doświadczeń użytkowników (10 proc.) oraz zarządzanie projektami (2,89 proc.).

33 PROC. POLAKÓW DEKLARUJE, ŻE JUŻ PODJĘŁO NAUKĘ ZAGADNIEŃ ZWIĄZANYCH Z IT

Na rynku jest bardzo bogata oferta dla tych, którzy myślą o edukacji w kierunku IT. Takie osoby mogą skorzystać nie tylko ze studiów kierunkowych, ale również odbyć liczne kursy i szkolenia. Ciekawą opcja są również bootcampy, które są organizowane przez firmy IT (czyli potencjalnych pracodawców). Nierzadko jest również tak, że firma organizująca taki bootcamp, po jego zakończeniu zatrudnia najzdolniejszych uczestników.

Polacy nie tylko myślą, ale i działają. ¼ Polaków deklaruje chęć przejścia do IT, ale jednocześnie już ⅓ z nas rozpoczęła edukację w tym obszarze. Dokładnie 35 proc. badanych przyznało, że jest w trakcie edukacji, a kolejne 35 proc. powiedziało, że jeszcze nie rozpoczęło nauki. Natomiast 31 proc. podejmowało naukę w obszarze IT w przeszłości.



Rocket Science Communications Successfully 360 PR agency for IT and Technology

ROCKET SCIENCE COMMUNICATIONS

Media Relations

Relacje z mediami w zakresie komunikacji produktowej, korporacyjnej, Employer Branding.

Kampanie

Prowadzenie kampanii digital, zakup mediów, influencer marketing.

Social Media

Prowadzenie kanałów na Facebooku, Twitterze, Instagramie.

Strategia

Przygotowanie, realizacja i egzekucja strategii komunikacji.

Na hasło "SecurityMagazine" bezpłatna konsultacja

www.rocketscience.com.pl

ZASILACZE AWARYJNE UPS W FIRMACH

Łukasz Toczek
MERIDO

Bezpieczeństwo IT na ogół kojarzy się z zabezpieczeniem sprzętu i oprogramowania przed nieautoryzowanym dostępem osób nieuprawnionych. Wszelkiego rodzaju oprogramowanie antywirusowe, firewalle, programy szyfrujące, bezpieczne bazy danych, zabezpieczone sieci wewnętrzne przychodzą na myśl naturalnie, gdy zaczynamy zastanawiać się nad tym zagadnieniem. W jego spektrum mieszczą się jeszcze inne mniej oczywiste rzeczy i nad jedną z nich pochylimy się w tym artykule.

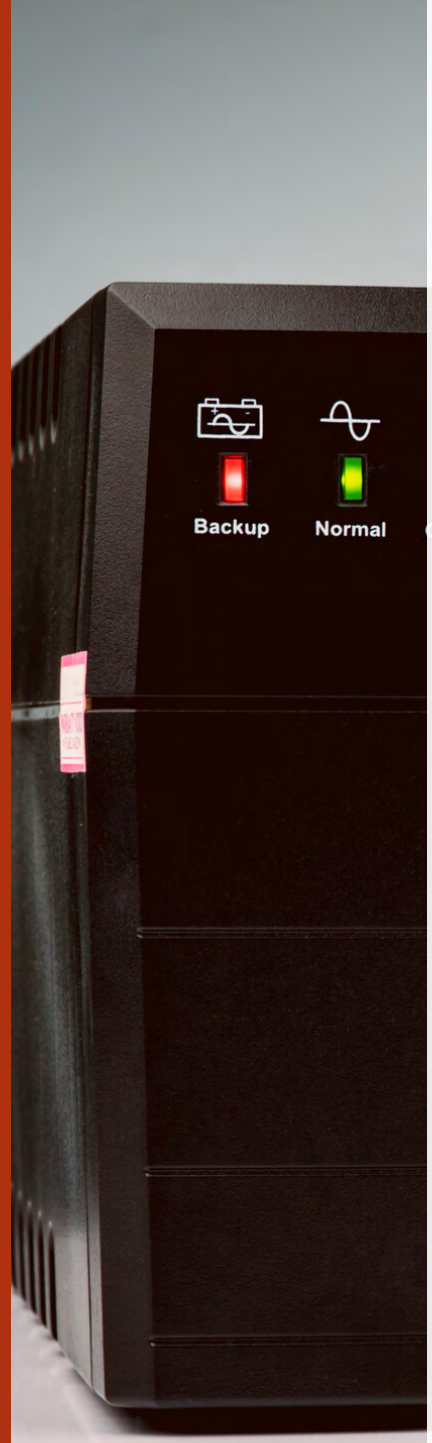
Co z tego, że mamy doskonale zabezpieczoną sieć, najlepsze oprogramowanie, przestrzegamy wszystkich zasad chroniących nas przed wyciekiem danych, jeśli możemy utracić efekty pracy w jednej chwili. Mówię tutaj o sprawie, wydawać by się mogło, banalnej, której konsekwencje mogą być nie do wycenienia. Przerwy w dostawie energii elektrycznej lub jej zakłócenia, bo o tym mowa, mogą odpowiadać za niewyobrażalne straty, jeśli podczas trwającej pracy utracimy niezapisane postępy. Przepięcie w sieci elektrycznej może doprowadzić do trwałego uszkodzenia delikatnego i nieraz bardzo kosztownego sprzętu elektronicznego. Nagły spa-dek napięcia może spowodować restarty całych systemów i uszkodzenia bazy danych.

Rozwiązanie oczywiście istnieje od dawna i jest już doskonale znane wśród osób i firm zajmujących się bezpieczeństwem w branży IT i nie tylko. Zasilacze awaryjne UPS. Być może kojarzą się z niepotrzebnym wydatkiem, wszak braki prądu nie są tak dotkliwe jak jeszcze kilkanaście lat temu. Warto jednak zauważyć, że w ostatnim czasie mamy coraz więcej gwałtownych i nieprzewidywalnych zdarzeń atmosferycznych, które mogą i często niosą za sobą chwilowe przerwy w dostawie energii.

Czasem są to tylko kilkusekundowe zaniki. Wystarczająco długo, by komputer się zrestartował.

Co wtedy? Wszystkie aplikacje są zamykane, tracimy kilka, czasem kilkanaście minut naszej pracy, przerywane są aktywne sesje internetowe. W ekstremalnych przypadkach może dojść do nieodwracalnych uszkodzeń baz danych, a ich zrestartowanie lub przywrócenie może trwać bardzo długo lub być niemożliwe.

W Merido od 25 lat zajmujemy się wsparciem medycyny i farmacji w zakresie oprogramowania, bezpieczeństwa systemów, baz danych oraz sprzętu: od zwykłych komputerów roboczych po serwery i urządzenia je zabezpieczające takie jak zasilacze awaryjne UPS właśnie. Sam temat jest bardzo szeroki i nie ma potrzeby omawiać każdej możliwej sytuacji, skupię się



na tym, czym zajmujemy się na co dzień i czym kierujemy się przy wyborze zasilaczy oraz jakie wymagania powinny spełniać, aby w pełni zabezpieczyć urządzenia, które mają chronić.

Na początek wyjaśnijmy jedną zasadniczą kwestię.
Zadaniem zasilacza awaryjnego nie jest umożliwienie długofalowej pracy podłączonych urządzeń (do tego służą agregaty prądotwórcze), a bezpieczne zakończenie aktualnie trwających procesów, zapisanie postępów prac i kontrolowane wyłączenie sprzętów do nich podłączonych. W związku z tym chronione są zazwyczaj kluczowe dla infrastruktury firmy urządzenia. Ze względu na koszty samych UPS-ów, po prostu nie opłaca się podłączać do nich innych sprzętów, bez których procesy zachodzące w firmie i tak będą funkcjonowały.

CZYM KIERUJEMY SIĘ PRZY WYBORZE ZASILACZA AWARYJNEGO?

Pierwsza odpowiedź, która mogłaby przyjść na myśl: cena - nie jest prawidłowa. Korzystamy ze sprawdzonych urządzeń renomowanych marek. Te, oczywiście, kosztują więcej, jednakże dają gwarancję niezawodności. Co w takim razie ma wpływ na wybór sprzętu dla klienta? To zależy, czego potrzebuje. Branża, której firmami się opiekujemy, ma swoją specyfikę. Apteki i placówki medyczne potrzebują stałego połączenia do internetu, aby móc realizować sprzedaż i obsługę pacjentów. Stała wymiana danych między stanowiskami, serwerem bazodanowym, a systemami zewnętrznymi jest tutaj kluczowa dla prawidłowego działania całego systemu obsługi pacjenta.

Do UPS-ów podłączone są zatem pojedyncze komputery, serwery i urządzenia sieciowe. W przypadku awarii związanej z dostawą energii elektrycznej zasilacze awaryjne przejmują na siebie ciężar utrzymania całej infrastruktury, dzięki czemu można bezpiecznie kontynuować rozpoczętą pracę przez co najmniej kilka minut.

Równie ważne jest to w przypadku chwilowych przerw w dostawie prądu, te dzięki wykorzystaniu zasilaczy awaryjnych mogą pozostać niezauważone. Jedynym sygnałem jest dźwięk informujący o uruchomieniu UPS-ów.

JAK DOBIERAMY ZASILACZE?

Tutaj zasada jest dosyć prosta. Kierujemy się maksymalnym poborem mocy urządzeń, które są podpięte do UPS-a i wybieramy taki, który ma jej odpowiedni zapas. Tak, żeby mieć kilka minut na bezpieczne wyłączenie sprzętów podtrzymywanych w tym czasie przez baterie zasilacza. Dla zwykłego stanowiska komputerowego i urządzeń sieciowych wystarczające są zasilacze 300-500W, dla serwera będzie to już powyżej 700W.

Mocnym uproszczeniem zasady wyboru mocy UPS-a jest: „im więcej, tym lepiej". Pewien rodzaj przewartościowania jest wskazany, ponieważ daje to zapas energii, a w przypadku wymiany podłączonych sprzętów na nowsze, często o zwiększonym poborze nie trzeba wymieniać samych zasilaczy. Należy natomiast pamiętać o monitorowaniu stanu akumulatorów i w razie potrzeby wymianie na nowe. Standardowo co 3-5 lat.

Korzystamy z urządzeń o topologii Line interactive, która charakteryzuje się nie tylko błyskawicznym przełączeniem na zasilanie bateryjne (4-12ms w zależności od modelu), ale stale monitorują napięcie, częstotliwość i kąt przesunięcia fazowego. Dzięki temu w momencie uruchamiania zasilania bateryjnego falownik synchronizuje się z siecią energetyczną. Przyspiesza to proces przełączania, co zapobiega pojawieniu się niepotrzebnych zakłóceń w podłączonych i często wrażliwych na tego typu sytuacje urządzeniach. Zasilacze są również wyposażone w system AVR, który służy, do korygowania poziomu napięcia zasilającego. Jeżeli to nieznacznie spada (lub rośnie), to przy pomocy układu jest korygowane, nie wymuszając jednocześnie uruchomienia się UPS-a.

DZIĘKI TEMU PRZY NIEZNACZNYCH WAHANIACH NAPIĘCIA MOŻEMY PRACOWAĆ, BEZ OBAW O POJEMNOŚĆ AKUMULATORA. TEN ZOSTANIE WYKORZYSTANY DOPIERO WÓWCZAS, GDY WAHANIA NAPIĘCIA BĘDĄ SPORE.

Rzadsze korzystanie z akumulatorów wydłuża ich żywotność, a wszystko dzięki AVR. Dodatkową zaletą zasilaczy Line interactive jest produkowanie napięcia lepszej jakości, bardziej zbliżonego do sinusoidalnego, albo w pełni sinusoidalnego, co daje możliwość wykorzystywania go do większej ilości urządzeń. W naszym przypadku nie ma to tak dużego znaczenia, ale warto o tym wspomnieć.

CZY WARTO?

Zdecydowanie. Obecnie wszystkie placówki pod naszą opieką są wyposażone w zasilacze awaryjne. Poczucie bezpieczeństwa i rzeczywiste zagwarantowanie go naszym klientom jest dla nas sprawą nadrzędną. Zabezpieczenie infrastruktury IT przed brakami prądu, gwałtownymi zmianami napięcia sieci elektrycznej znacząco przyczynia się do stabilności pracy sprzętu i systemów. Dodatkowo minimalizując ryzyko uszkodzenia urządzeń i danych.

MERIDO®

OPROGRAMOWANIE DLA MEDYCYNY I FARMACJI

„ZAOPIEKUJEMY SIĘ TWOIM BIZNESEM, ABYŚ MÓGŁ ZADBAĆ O ZDROWIE INNYCH”

RZESZÓW, UL. WITA STWOSZA 64

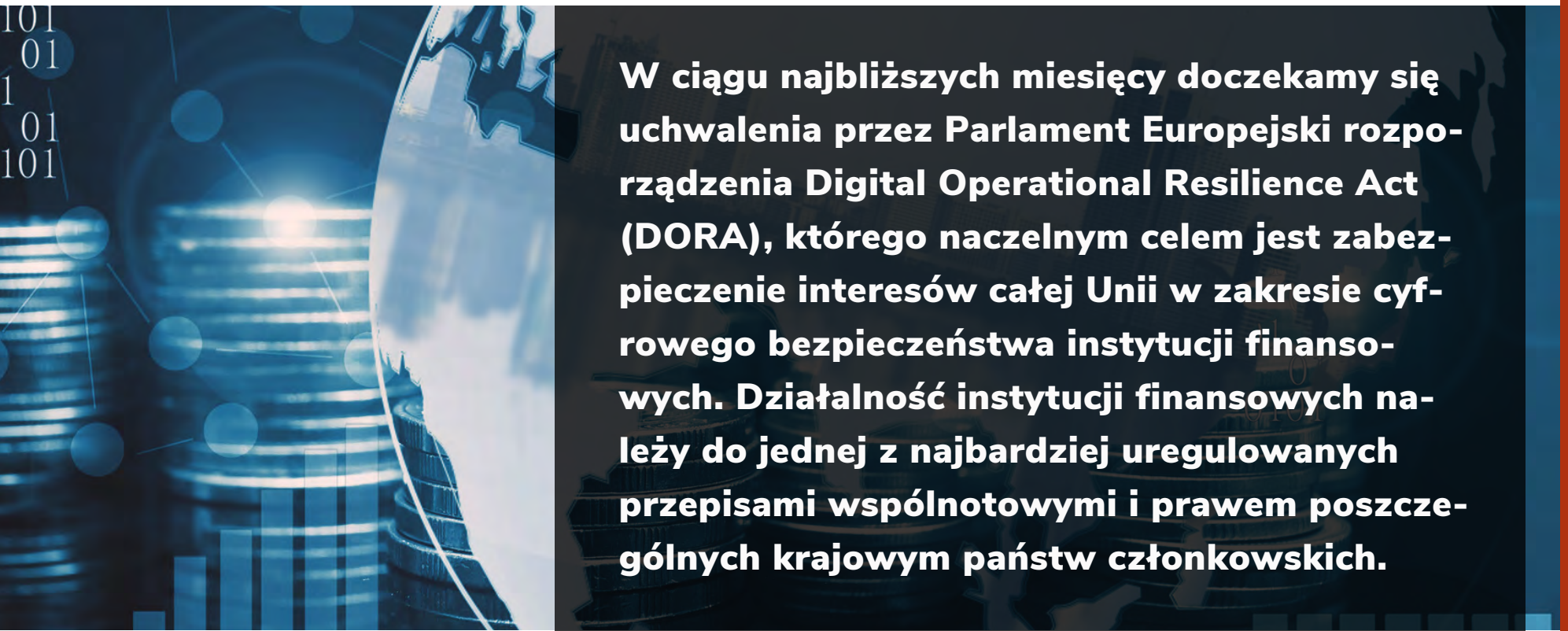
E-MAIL: merido@merido.pl

TEL. 17 864 02 40

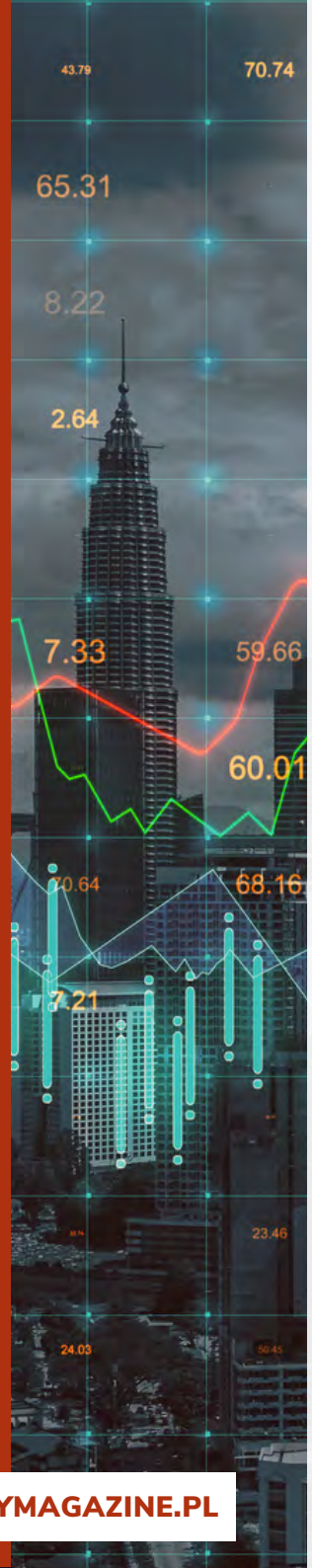
WWW.MERIDO.PL

CYBERBEZPIECZEŃSTWO INSTYTUCJI FINANSOWYCH W ŚWIETLE REGULACJI DORA

sier. Paweł Ładna



W ciągu najbliższych miesięcy doczekamy się uchwalenia przez Parlament Europejski rozporządzenia Digital Operational Resilience Act (DORA), którego naczelnym celem jest zabezpieczenie interesów całej Unii w zakresie cyfrowego bezpieczeństwa instytucji finansowych. Działalność instytucji finansowych należy do jednej z najbardziej uregulowanych przepisami wspólnotowymi i prawem poszczególnych krajowym państw członkowskich.



Jest to zrozumiałe, biorąc pod uwagę ich rolę we współczesnym świecie oraz fakt, iż przechowują ogromne ilości danych wrażliwych oraz danych finansowych. Jeszcze przed lutym 2020 roku zauważono, że nawet pojedynczy incydent cyberbezpieczeństwa może spowodować kryzys, który może zagrozić stabilności europejskiego systemu finansowego, dlatego podjęto działania mające na celu stworzenie DORA. Regulacja wymusi zmiany i ujednolici kwestie ryzyk, zarządzania ryzykiem oraz incydentami bezpieczeństwa dla wszelkich instytucji finansowych działających na obszarze UE.

Obecnie organizacje polegają na własnych systemach bezpieczeństwa i same określają, które systemy są krytyczne, a które nie. Ponadto jeśli te systemy są zarządzane przez zewnętrznych dostawców, organizacja zadowala się jedynie warunkami umowy, częściowo zrzucając odpowiedzialność za bezpieczeństwo na dostawcę usług i jego zapewnienia. W przypadku organizacji składających się z wielu mniejszych podmiotów, także spoza UE, brak jednolitych standardów, może stanowić punkt wejścia dla ataku na systemy organizacji i dostęp do danych, które normalnie nie opuszczają strefy UE (np. dane osobowe określone w GDPR).

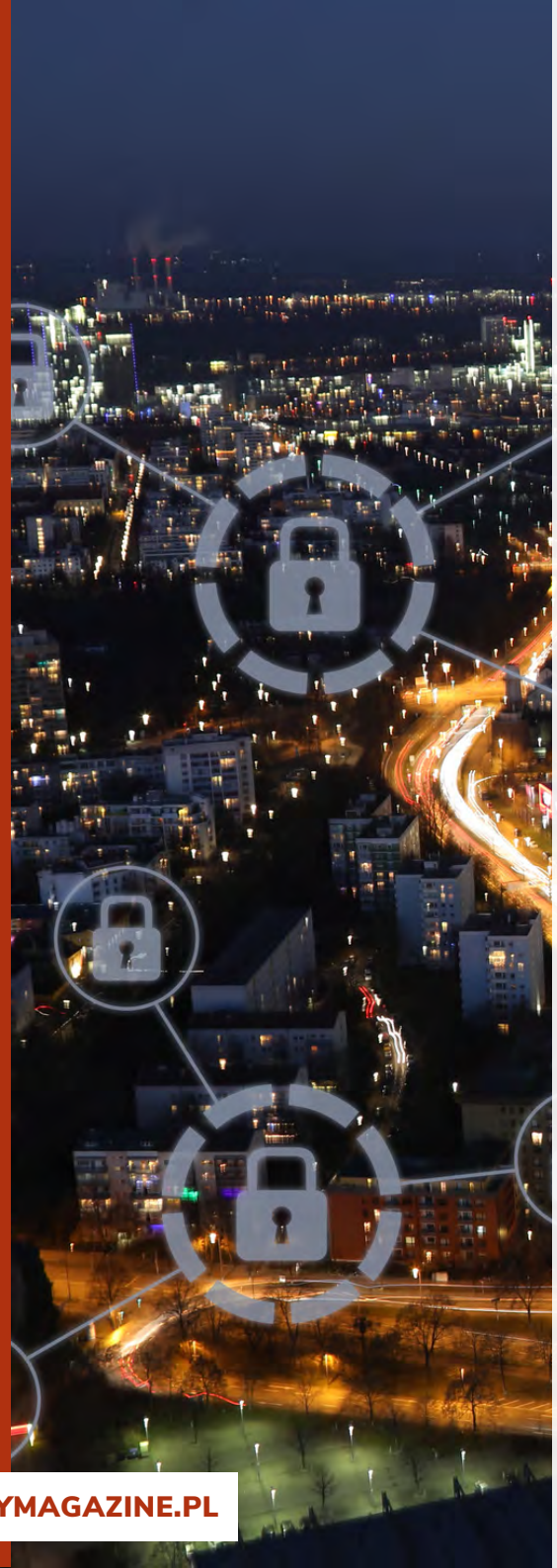
Aktualnie w praktyce istnieją już pewne uniwersalne standardy, ale ich stosowanie jest zależne od państw członkowskich. I tak, Litwa nakazuje instytucjom finansowym podążanie za wskazówkami wydanymi przez European Bank Authority (EBA), podczas gdy **Polska Komisja Nadzoru Finansowego stosuje jedynie część z nich. Brak jednolitej ramy bezpieczeństwa, sprawia, że pojedyncze kraje mogą stanowić wektor ataku i faktycznie zdestabilizować systemy połączone, jakimi są finanse.**

CZYM WIĘC JEST DORA?

To projekt regulacji, której wstępna wersja powstała już we wrześniu 2020 roku. Ma ona na celu ujednolicenie części aktów regulacyjnych, podniesienie kompetencji organów europejskich i umożliwienie im większej kontroli nad bezpieczeństwem instytucji finansowych oraz wymuszenie zmian i ujednolicenie zarządzaniem ryzykiem w segmencie finansowym. **Regulacja będzie miała wpływ między innymi na instytucje kredytowe, inwestycyjne, transferów elektronicznych, dostawców serwisów typu Crypto-assets, szeroko pojętego tradingu, alternatywnych funduszy inwestycyjnych, towarzystw ubezpieczeniowych, instytucji emerytalnych, agencji ratingu kredytowego, audytorów i serwisów typu crowdfunding.**

Mimo szerokiego zakresu dokumentu, wpływa dość głęboko na pewne istotne aspekty cyberbezpieczeństwa w tych organizacjach:

- **Zarządzanie ryzykiem:** Organizacje będą musiały stworzyć i utrzymać odporne (resilient) systemy i powiązane z nimi narzędzia, pozwalające na identyfikację i minimalizacje potencjalnego ryzyka. Systemy te będą musiały być stale utrzymywane i aktualizowane, aby utrzymać pewien podstawowy poziom bezpieczeństwa, posiadać systemy zapobiegawcze i jasno określone, sformalizowane polityki i plany dotyczące ciągłości biznesowej oraz planów odbudowy. Ideą regulacji jest ścisłe powiązanie strategii instytucji finansowych z zarządzaniem ryzykiem ICT. Współczesne standardy cyberbezpieczeństwa obejmują takie założenia jak identyfikacja, protekcja, prewencja, wykrywanie, odpowiedź i powrót do normalności (recovery), a także świadomość i komunikację, dlatego regulacja nie precyzuje własnych. Zamiast tego **organizacje będą odpowiedzialne za stałe monitorowanie swoich ryzyk w zakresie ICT a także zobowiązane podejmować odpowiednie czynności naprawcze i mitygacyjne.** Dodatkowym aspektem jest to, że DORA stawia duży nacisk na świadomość (awareness) użytkowników, szkolenia i ewolucję procesów zbierania informacji oraz działań po incydentach (analiza post-incydentalna, analiza procesu po incydencie, komunikacja). Wszystkie powyższe działania muszą być jasno określone i komunikowane klientom i publicznie.



Raportowanie incydentów: Niezbędne będzie ustalenie formalnego procesu informowania i raportowania o incydentach bezpieczeństwa. Incydenty będą musiały być monitorowane, a istotniejsze naruszenia raportowane do odpowiednich kompetentnych organów lokalnych. Jest to rozwinięcie już istniejącego TIBER-EU, czyli ram dla threat intelligence oraz dla red teamów. Kompatybilność z NIST sprawia, że organizacje posiadają jasny zestaw standardów i możliwość stałego zwiększania swojej dojrzałości w zakresie bezpieczeństwa. Oczywiście, nasuwa się pytanie, jakie będą kryteria klasyfikacji istotności incydentów. Te zostały przybliżone w Artykule 16 regulacji, jednocześnie określając, że ESA z European Central Bank (ECB) oraz European Union Agency for Cybersecurity (ENISA), stworzą spójny standard do wykorzystania w przyszłości.

Testowanie cyfrowej odporności: Organizacje będą zobowiązane do przeprowadzania pentestów i monitorowania funkcjonalności operacyjnej ich rozwiązań ICT pod kątem ram zarządzania (management framework), identyfikacji podatności i braków. Zakres minimalnych testów został zdefiniowany, tak aby brać pod uwagę oceny podatności, analizy rozwiązań otwarto źródłowych (open source), oceny bezpieczeństwa sieci, analiza luk (gap analysis), bezpieczeństwo fizyczne, a także analizy oprogramowania (analizy kodów źródłowych, testy oparte na scenariuszach, testy kompatybilności, wydajności oraz testy penetracyjne). Należy zaznaczyć, że zgodnie z zasadą proporcjonalności, zaawansowane testowanie będzie obligatoryjne jedynie dla instytucji określonych przez zewnętrzne kompetentne organy jako istotne (wg. kryteriów określonych przez ESA).

Zarządzanie przez zewnętrznych dostawców: To jeden z głównych obszarów regulacji. Obecnie usługi lub produkty stworzone przez zewnętrznych dostawców opierają się na kontrakcie, a odpowiedzialność za jakość przesuwana jest na dostawcę.

DORA znacząco zmienia ten stan rzeczy, wskazując minimalne wymagania kontraktów, a także nakazując, aby elementy krytyczne podlegały nadzorowi także przez organy unijne (najczęściej mówi się o European Supervisory Authorities - ESA, która będzie mogła uzyskać wgląd do dokumentacji, przeprowadzać inspekcje, a nawet nakładać kary finansowe).

Oznacza to, że jeśli organizacja uznaje za infrastrukturę krytyczną jej fragment zarządzany przez dostawców (np. rozwiązania chmurowe, zewnętrzne SOC/SIEM), to dostawca będzie podlegał kontroli organom EU.

Rozwiązanie będzie szczególnie istotne dla organizacji, które posiadają aktywa poza terenem Unii i nie podlegają prawodawstwu EU.

Przykład z mojego doświadczenia zawodowego pokazuje, że jedna z firm spoza Europy, należąca do europejskiego holdingu, stanowi istotne ryzyko dla danych osobowych. Niepodlegające GDPR dane osobowe są przechowywane bez anonimizacji i bezterminowo, jednocześnie dojrzałość w zakresie bezpieczeństwa ICT tej firmy jest niska. Łatwo wyobrazić sobie scenariusz, w którym może ona zostać wykorzystana jako punkt wejściowy, aby uzyskać dostęp do zuni-

fikowanych systemów holdingu. Przypadki ataków według wskazanego scenariusza występowały już w praktyce, należy także brać pod uwagę, że współczesne konflikty, w tym wojna w Ukrainie, toczą się równolegle w świecie rzeczywistym oraz w cyberprzestrzeni. Takie podatności, jeśli zauważone, mogą stanowić punkt ataku na instytucje i obywateli Unii Europejskiej. Konieczność poddania się kontrolom oraz możliwe kary mogą wymusić, aby te same standardy były przestrzegane niezależnie od lokalizacji firmy, co jest częstym problemem w międzynarodowych organizacjach.

Jak łatwo zauważyć, niektóre instytucje już posiadają wszystkie lub szereg wymaganych rozwiązań, choć zapewne dotyczy to w większości dużych i dojrzałych organizacji. Regulacja, podobnie jak wcześniej GDPR, załata luki i dziury w mniejszych organizacjach, narzucając jednolity standard, rozwiązania i minimalny poziom bezpieczeństwa. Oczywiście, nierozwiązanym problemem wciąż pozostają braki specjalistów oraz koszty przedsięwzięcia. Wiele mniejszych firm nie będzie w stanie zbudować własnego SOC, więc będą musiały polegać na zewnętrznych dostawcach.

Podsumowując, DORA jest więc pewnego rodzaju kompilacją i ujednoliceniem już istniejących regulacji, dostosowaną do nowoczesnych standardów i narzucających stałą kontrolę i nadzór nad cyberbezpieczeństwem sektora finansowego. Jest efektem powolnego, ale stałego dojrzewania Unii do większej i bardziej jednolitego nadzoru wspólnego nad bezpieczeństwem sektora finansowego. Początkowo będzie stanowić wyzwanie, jednak trudno nie docenić jej holistycznego podejścia do cyberbezpieczeństwa i roli w zabezpieczeniu słabych punktów sektora finansowego.

Analizy jednej z największych firm konsultingowych wskazują, że zdecydowana większość instytucji przywita regulacje z otwartymi ramionami, traktując ją jako dodatkowe potwierdzenie ich stabilności, a także zachęci je do większego inwestowania w rozwiązania chmurowe.

Pierwsza propozycja DORA została opublikowana we wrześniu 2020 roku, zazwyczaj taka regulacja zostaje przyjęta w czasie 12-18 miesięcy, jednak pandemia spowodowała znaczne opóźnienie we wprowadzaniu jej w życie.

Obecna sytuacja polityczna może być motorem do wprowadzenia jej w życie - w związku z agresją Rosji na Ukrainę oraz zwiększoną ilością ataków cybernetycznych (wielu także ze strony rosyjskiej), wiele organizacji już teraz modyfikuje swoje zabezpieczenia, a wprowadzenie przez Unię Europejską DORA leży w interesie europejskiej strefy gospodarczej oraz sektora finansowego.


/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

CHCESZ KORZYSTAĆ Z FACE RECOGNITION? OTO WARUNKI, NA JAKICH MOŻESZ TO ZROBIĆ

Redakcja
SECURITY MAGAZINE

W ubiegłym roku Komitet Konwencji nr 108 Rady Europy o ochronie osób w związku z coraz częstszym stosowaniem technologii rozpoznawania twarzy przyjął „Wytyczne dotyczące rozpoznawania twarzy". Teraz są one dostępne również w naszym języku. Przygotowaliśmy najważniejszy skrót informacji zawartych w "Wytycznych", które każdy podmiot publiczny i prywatny musi znać.

„Wytyczne dotyczące rozpoznawania twarzy" były kwestią czasu w dobie coraz powszechniej stosowanej technologii rozpoznawania twarzy. Mają one na celu zapewnić zgodność m.in. z prawem ochrony danych osobowych. Nad samymi przepisami Unia Europejska pracuje od 3 lat i są to pierwsze takie przepisy na świecie.

- Dzięki nim Unia Europejska obejmuje pozycję lidera w dziedzinie opracowywania nowych, globalnych norm – powiedziała **komisarz UE ds. cyfryzacji Marghrete Vestager.**

EUROPEJSKIE WYTYCZNE DOTYCZĄCE ROZPOZNAWANIA TWARZY

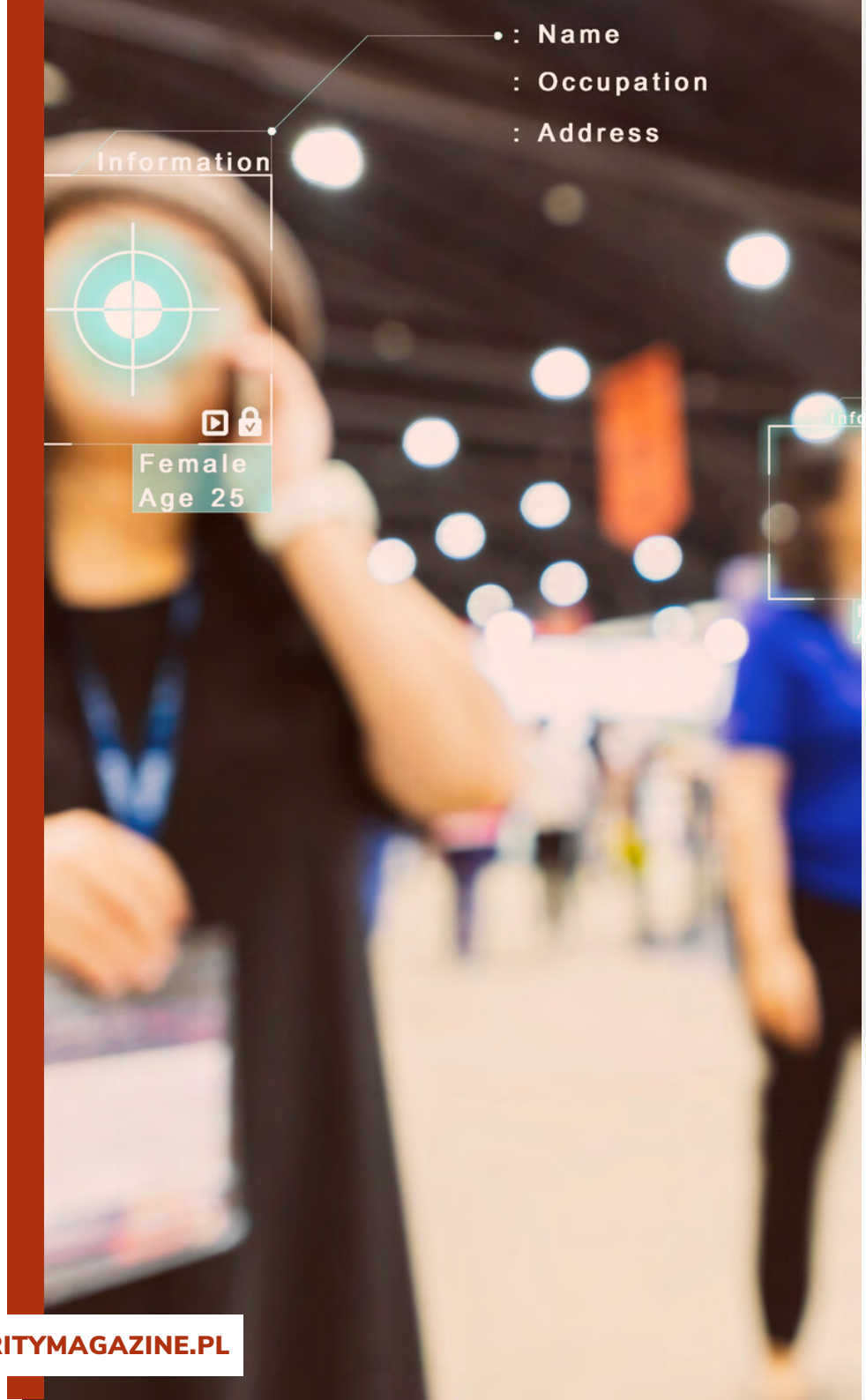
Jak wspomnieliśmy, jest już ich polska wersja, z którą może zapoznać się każdy przedsiębiorca, ciekawy rozwiązań prawnych w kontekście tej technologii czy ten który już wprowadził lub będzie chciał prowadzić do swojej działalności face recognition.

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

OTO, CO MUSISZ WIEDZIEĆ O ROZPOZNAWANIU TWARZY Z "WYTYCZNYCH"

Integracja technologii rozpoznawania twarzy jest zagrożeniem dla prawa do prywatności i ochrony danych osobowych, dlatego, że korzystanie z niej nie zawsze wymaga świadomości czy współpracy osób, do których należą przetwarzane dane biometryczne.

Chcesz korzystać z Face recognition? Oto warunki, na jakich możesz to zrobić



Dlatego tak ważne jest zapewnienie, że rozwój i wykorzystywanie tej technologii będą prowadzone z poszanowaniem prawa do prywatności i ochrony danych, prawa człowieka i wolności. Co za tym idzie, przetwarzanie w szczególności danych biometrycznych, jest dozwolone wyłącznie wtedy, gdy opiera się ono na odpowiedniej podstawie prawnej.

Rozpoznawanie twarzy powinno być zabronione, jeśli służyć ma jedynie do określenia: koloru skóry, przekonań religijnych lub innych, pochodzenia rasowego lub etnicznego, wieku, stanu zdrowia lub stanu społecznego danej osoby, płci, a nawet emocji, cech osobowości, uczuć, zdrowia psychicznego lub zaangażowania pracowników na podstawie obrazów twarzy.

- *Powiązanie rozpoznania emocji, np., z zatrudnianiem personelu, dostępem do ubezpieczenia, edukacją, może stanowić poważne zagrożenie, zarówno na poziomie indywidualnym, jak i społecznym, i powinno być zabronione* - czytamy w polskiej wersji „Wytycznych dotyczących rozpoznawania twarzy", które zostały podzielone na dwie części ze względu na to, jak face recognition ma traktować sektor publiczny, a jak prywatny.

Zasady dla sektora publicznego, który wykorzystuje rozpoznawanie twarzy:

- Zgoda **nie powinna stanowić podstawy prawnej** do korzystania z tej technologii ze względu na brak równowagi uprawnień między osobami, których dane dotyczą, a organami publicznymi (w RODO podobny zapis znajdziemy w motywie 43).
- Zasady dotyczące przetwarzania danych **muszą być szczegółowo określone przez ustawodawców** i decydentów, by móc je prawnie egzekwować.
- Musi istnieć **wyraźna i precyzyjna podstawa prawna** zapewniająca niezbędne zabezpieczenia przetwarzania danych biometrycznych.

Zasady dla sektora prywatnego, który wykorzystuje rozpoznawanie twarzy:

- Osoby, których dane dotyczą i których dane biometryczne są przetwarzane **muszą wyrazić na to zgodę** wyraźną, konkretną, dobrowolną i świadomą.
- Aby zgoda była dobrowolna, **trzeba zapewnić osobom, których dane dotyczą, alternatywę rozwiązania** w stosunku do korzystania z technologii rozpoznawania twarzy (na przykład za pomocą hasła lub identyfikatora).
- Alternatywy te mają być **łatwe w użyciu**, ponieważ jeżeli byłyby zbyt skomplikowane w porównaniu z technologią rozpoznawania twarzy, wybór nie byłby prawdziwy.
- Podmioty prywatne **nie mogą wdrażać rozpoznawania twarzy w niekontrolowanych środowiskach**, takich jak centra handlowe, zwłaszcza w celu identyfikacji osób będących przedmiotem zainteresowania, do celów marketingowych lub do celów bezpieczeństwa prywatnego.

Wymagane jest zaangażowanie organów nadzorczych do konsultowania spraw ewentualnych eksperymentów lub przewidywanego zastosowania.

W związku z tym konsultacje mają być systematyczne i przed planowanymi projektami. Organy powinny mieć dostęp do przeprowadzonych ocen skutków, do wszystkich audytów, sprawozdań i analiz przeprowadzonych w kontekście takich eksperymentów lub projektów.
Twórcy, producenci, usługodawcy i podmioty korzystające z rozpoznawania twarzy powinni być rozliczani ze stosowanych technologii.

- *Ustanowienie niezależnego ii kwalifikowanego mechanizmu certyfikacji w zakresie rozpoznawania twarzy i ochrony danych w celu wykazania pełnej zgodności prowadzonych operacji przetwarzania byłoby podstawowym elementem bu-dowania zaufania użytkowników* - czytamy w “Wytycznych”.

Ponadto podmioty te powinny zapewnić dostęp do prostych pojęć, które mogłyby ostrzec osoby, których dane dotyczą, zanim zdecydują się na skorzystanie z technologii rozpoznawania twarzy, aby zrozumieć, co to znaczy wykorzystywać dane wrażliwe, takie jak dane biometryczne, jak działa rozpoznawanie twarzy, oraz ostrzec je o potencjalnym niebezpieczeństwie, zwłaszcza w przypadku niewłaściwego wykorzystania.

Komitet Konwencji nr 108 Rady Europy opracował wytyczne dla twórców, producentów i dostawców usług. Będą musieli oni unikać błędnego etykietowania, a tym samym wystarczająco testować swoje systemy oraz identyfikować i eliminować rozbieżności w prawidłowości, a tym samym unikać niezamierzonej dyskryminacji.

Ważne jest, by przewidzieć procedury awaryjne na wypadek awarii systemu, a dane biometryczne jak informacje o rodzaju choroby, niepełnosprawności fizycznej, musiałyby podlegać uzupełniającym odpowiednim zabezpieczeniom.

W opracowywaniu i sprzedaży technologii face recognition firmy muszą wziąć pod uwagę:

- włączenie ochrony danych w projekt
- zaoferowanie elastyczności zgodnie z zasadami ograniczenia celu, minimalizacji danych i ograniczenia czasu przechowywania danych
- określenie i zminimalizowanie potencjalnego wpływu na prawa i podstawowe wolności, zanim technologie rozpoznawania twarzy staną się dostępne
- przydzielenie dedykowanego personelu, zapewnienie pracownikom szkolenia w zakresie ochrony prywatności oraz przeprowadzanie ocen skutków dla ochrony danych.

Komitet Konwencji nr 108 Rady Europy opracował również wytyczne dla podmiotów wykorzystujących technologie rozpoznawania twarzy. Firmy te muszą być w stanie wykazać, że ich zastosowanie jest ściśle niezbędne i proporcjonalne w określonym kontekście ich stosowania oraz że nie narusza praw osób, których dane dotyczą.

To, jakim regulacjom prawnym będą podlegać, zależeć będzie od ich sektorów i celów stosowania technologii, a w przetwarzaniu danych kluczowe będą:

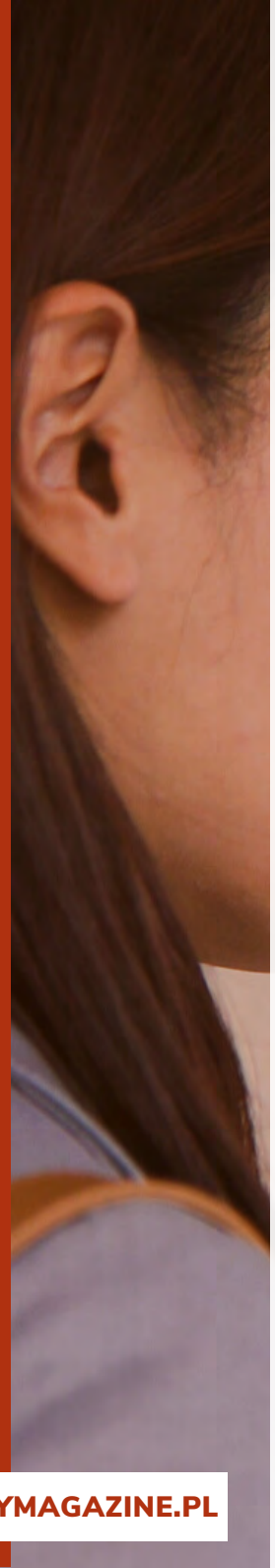
1. **Przejrzystość i rzetelność** - obejmują m.in. to, czy informacje są przekazywane osobom fizycznym, kontekst zbierania danych, rozsądne oczekiwania co do sposobu wykorzystania danych, czy rozpoznawanie twarzy jest jedynie cechą produktu lub usługi czy raczej integralną częścią samej usługi. Przekazane informacje muszą również określać, jakie prawa i środki ochrony prawnej przysługują osobom, których dane dotyczą.
2. **Ograniczenie celu, minimalizacja danych i ograniczenie czasu przechowywania** - dane osobowe podlegające przetwarzaniu powinny być zbierane w wyraźnych, konkretnych i prawnie uzasadnionych celach. Ponadto, przed jakimkolwiek kolejnym przetwarzaniem podmioty musiałyby rozważyć, czy cele nowego przetwarzania są zgodne z celami pierwotnie określonym. W przeciwnym razie nowe przetwarzanie będzie wymagało odrębnej podstawy prawnej. Zasada minimalizacji danych wymagałaby, aby przetwarzane były tylko niezbędne informacje, a nie wszystkie informacje dostępne podmiotom. Co do ograniczenia czasu to okres zatrzymywania danych nie może być dłuższy niż okres niezbędny do konkretnego celu przetwarzania. Firmy muszą również zapewnić usunięcie szablonów biometrycznych po zakończeniu celu.
3. **Prawidłowość** - jakość obrazów i szablonów biometrycznych umieszczonych na listach obserwacyjnych musi być sprawdzona, aby zapobiec potencjalnym fałszywym dopasowaniom. Niska jakość obrazów może spowodować wzrost liczby błędów. W przypadku błędnych dopasowań

podmioty muszą podjąć wszelkie uzasadnione kroki w celu skorygowania przyszłych zdarzeń oraz zapewnienia prawidłowości obrazów cyfrowych i szablonów biometrycznych.

Bezpieczeństwo to priorytet przy wdrażanych technologiach face recognition.

- Należy wdrożyć silne środki bezpieczeństwa, zarówno na poziomie technicznym, jak i organizacyjnym, w celu ochrony danych dotyczących rozpoznawania twarzy i zestawów obrazów przed utratą i nieuprawnionym dostępem lub wykorzystaniem danych na wszystkich etapach przetwarzania, niezależnie od tego, czy chodzi o zbieranie, przekazywanie i przechowywanie - czytamy w “Wytycznych”.

Podmioty będą musiały podjąć działania mające na celu zapobieganie atakom specyficznym dla technologii, w tym atakom prezentacyjnym (związane z lukami czysto biometrycznymi. Intruzi używają pewnego rodzaju artefaktów, zwykle sztucznych lub próbują naśladować wygląd prawdziwych użytkowników w celu uzyskania fałszywego dostępu do systemu biometrycznego) i atakom morfingu (podszywanie się pod osobę celem uzyskania fałszywego dostępu do urządzeń, do których dostęp uzyskujemy przez biometrię twarzy). - *Każde naruszenie bezpieczeństwa danych, które może poważnie kolidować z prawami i podstawowymi wolnościami osób, których dane dotyczą, musi zostać zgłoszone organowi nadzorczemu oraz, w stosownych przypadkach, osobom, których dane dotyczą - cytujemy "Wytyczne dotyczące rozpoznawania twarzy."*



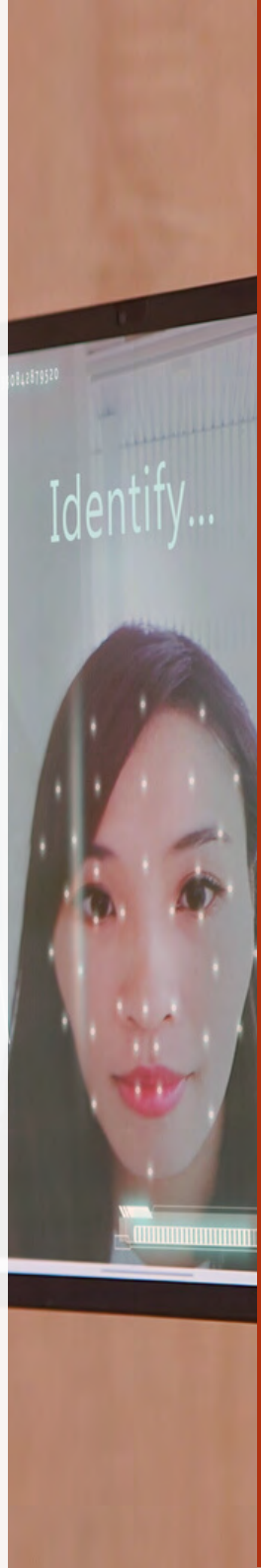
Warto wiedzieć, że podmioty stosujące technologie rozpoznawania twarzy muszą uwzględnić następujące środki organizacyjne:

- Wdrażanie przejrzystych polityk, procedur i praktyk w celu zapewnienia, że ochrona praw osób, których dane dotyczą, leży u podstaw stosowania przez nie technologii rozpoznawania twarzy
- Publikowanie sprawozdań na temat przejrzystości dotyczących konkretnego wykorzystania technologii rozpoznawania twarzy
- Ustanawianie i dostarczanie programów szkoleniowych i procedur audytu dla osób odpowiedzialnych za przetwarzanie danych dotyczących rozpoznawania twarzy
- Ustanawianie wewnętrznych komitetów weryfikacyjnych w celu oceny i zatwierdzania wszelkiego przetwarzania danych dotyczących rozpoznawania twarzy
- Umowne rozszerzenie odpowiednich wymogów na dostawców usług będących stronami trzecimi, partnerów biznesowych lub inne podmioty wykorzystujące technologię rozpoznawania twarzy (oraz odmowa dostępu stronom trzecim, które by ich nie przestrzegały).

UWAGA! Podmioty wykorzystujące technologie rozpoznawania twarzy muszą zagwarantować, że ludzie jako operatorzy będą nadal odgrywać decydującą rolę w działaniach podejmowanych w oparciu o wyniki tych technologii.

ETYKA

"Wytyczne" zamyka aspekt etyczny technologii face recognition. - *Aby uniknąć łamania praw człowieka, komitety ekspertów z różnych dziedzin będą prawdopodobnie definiować najtrudniejsze przypadki wykorzystania technologii rozpoznawania twarzy. W tej kwestii istotną rolę do odegrania mają również sygnaliści, a pracownicy podmiotów korzystających z tych rozwiązań powinni mieć możliwość korzystania z odpowiedniego statusu ochrony* - czytamy.



Chcesz korzystać z Face recognition? Oto warunki, na jakich możesz to zrobić

Wszystkie prawa przewidziane w Konwencji 108 są zagwarantowane osobom, których dane dotyczą, a są to:

- prawo do informacji,
- prawo dostępu,
- prawo do zapoznania się z uzasadnieniem,
- prawo do sprzeciwu,
- prawo do sprostowania danych.

W przypadku fałszywych dopasowań, osoby, których dane dotyczą, mogą zażądać sprostowania, aby uniknąć kolejnych czy powtarzających się sytuacji.

W TWOJEJ FIRMIE
ZDARZYŁ SIĘ

WYCIEK DANYCH OSOBOWYCH?

MOŻEMY CI POMÓC

SPRAWDŹ JAK

Polityka® Bezpieczeństwa

SECURITYMAGAZINE.PL

ZNACZENIE WYROKU SCHREMS II DLA TRANSFERU DANYCH OSOBOWYCH

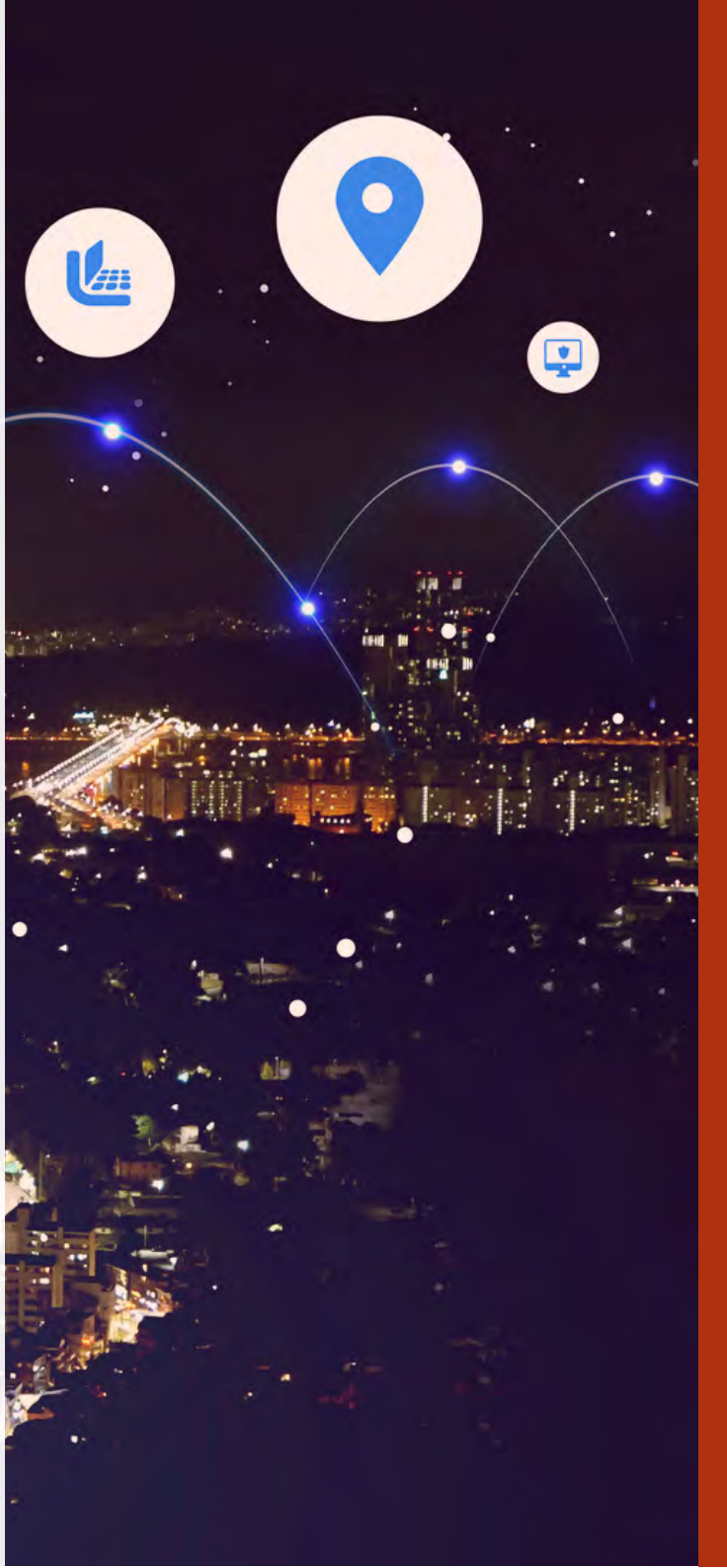
Wojciech Świątek
EY

Ochrona danych osobowych to specyficzne zadanie, z jakim mierzą się organizacje na całym świecie. W dobie ciągłego rozwoju technologii zapewnienie bezpieczeństwa danych związane jest ze stosowaniem skutecznych środków i zachowaniem wymogów wynikających z aktów prawnych.

Szczególnie istotne jest właściwe zabezpieczenie danych osobowych w przypadku ich transferu z Unii Europejskiej do państw trzecich. **Na gruncie przepisów dotyczących ochrony danych osobowych przyjęło się określać pojęciem „państwa trzecie" terytoria znajdujące się poza tzw. Europejskim Obszarem Gospodarczym, tworzonym przez Unię Europejską oraz trzy kraje: Islandię, Norwegię i Liechtenstein.** W kwestii przekazywania danych do państw trzecich przełomową rolę odegrał wyrok Schrems II wydany przez Trybunał Sprawiedliwości Unii Europejskiej. Na jego mocy uchylono akt będący podstawą prawną przekazywania danych osobowych pomiędzy Unią Europejską a Stanami Zjednoczonymi Ameryki Północnej, czyli decyzję wykonawczą Komisji Europejskiej, która wprowadzała tzw. **Tarczę Prywatności** - instrument zapewniający legalność transferu danych. Orzeczenie to wywołało konsekwencje nie tylko o charakterze normatywnym, ale również organizacyjnym.

ETAPY ZAPEWNIENIA ZGODNOŚCI Z UNIJNYM POZIOMEM OCHRONY DANYCH OSOBOWYCH W ORGANIZACJI

Konsekwencją wyroku okazała się przede wszystkim konieczność zapewnienia odpowiedniego zabezpieczenia w przypadku transferu danych osobowych. Poziom ochrony danych musi odpowiadać temu, który zapewniany jest w Unii Europejskiej. W związku z tym powinnością spoczywającą na każdej organizacji w kontekście orzeczenia wydanego przez TSUE jest wdrożenie odpowiednich zmian wynikających z konieczności zapewnienia odpowiedniego poziomu ochrony danych osobowych w przypadku przekazywania ich do państw trzecich.



Pierwszym etapem zapewnienia zgodności z unijnym poziomem ochrony danych osobowych w organizacji jest identyfikacja transferu danych. Podmiot eksportujący powinien dokonać rozpoznania i rejestracji wszel-kich przeprowadzonych operacji przekazywania danych. Mogą one zos-tać zweryfikowane np. w oparciu o tzw. rejestry czynności przetwarzania danych osobowych.

Drugi etap zapewnienia zgodności poziomu ochrony danych osobowych w organizacji z poziomem gwarantowanym w Unii Europejskiej polega na sprawdzeniu legalności transferu tych danych. W tym kontekście istotne jest zweryfikowanie, czy narzędzie stanowiące podstawę przekazywania danych, zostało wskazane w przepisach RODO. Po pierwsze, stosownie do treści przepisów transfer danych może nastąpić wówczas, gdy Komisja Europejska stwierdzi zapewnienie odpowiedniego poziomu ochrony danych osobowych w państwie trzecim bądź na określonym jego terytorium lub sektorze albo w organizacji międzynarodowej i wyda decyzję wykonawczą w przedmiotowej kwestii.

Każdy podmiot dokonujący transferu danych osobowych jest obowiązany do przeprowadzenia analizy porządku prawnego państwa trzeciego będącego odbiorcą tych danych oraz praktyk podejmowanych w tym państwie. Analizie tej towarzyszyć musi ocena wpływu regulacji na skuteczność narzędzia wykorzystywanego do przekazywania danych osobowych.

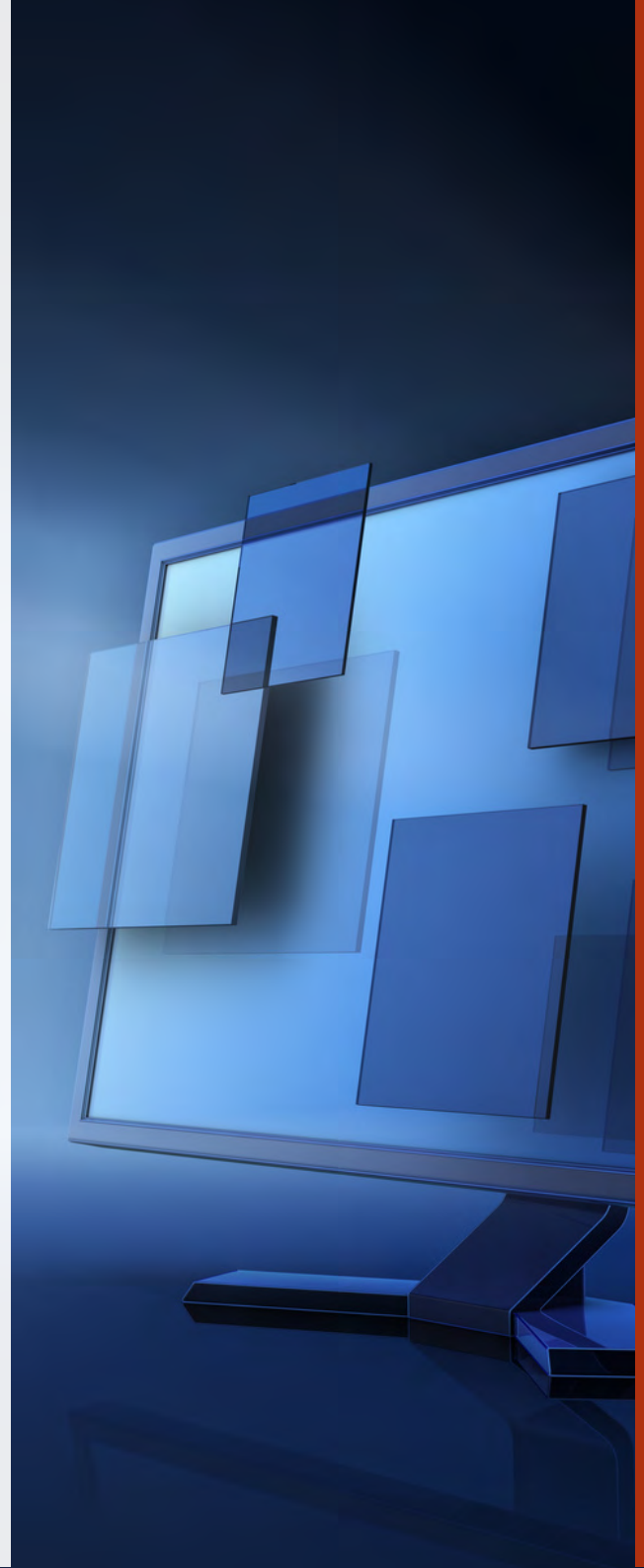
Niewątpliwie etap ten jest najbardziej wymagający spośród wszystkich, ponieważ polega nie tylko na zapoznaniu się z reżimem prawnym państwa trzeciego

w aspekcie ochrony danych osobowych, ale również jego dogłębnej analizie, która pozwoli na stwierdzenie, czy zastosowane narzędzie będące podstawą transferu nie zostanie pozbawione skuteczności na mocy konkretnego przepisu czy praktyki oraz bieżącym monitorowaniu zmian w obowiązującym ustawodawstwie.

Kolejnym etapem zapewnienia zgodności z unijnym poziomem ochrony danych osobowych w organizacji, czyli wdrożenia zasady rozliczalności w praktyce, jest określenie, za pomocą jakich narzędzi odbywa się przekazywanie danych osobowych. Do dyspozycji administratora danych bądź podmiotu przetwarzającego przewidziane są dwa rodzaje narzędzi: decyzja, na mocy której Komisja UE stwierdza odpowiedni stopień ochrony danych oraz narzędzia przekazywania wskazane w art. 46 RODO.

ŚRODKI UZUPEŁNIAJĄCE NARZĘDZIA PRZEKAZYWANIA DANYCH

Od wyniku oceny narzędzi wykorzystywanych w procesie przekazywania danych osobowych w organizacji zależy, czy będzie konieczne zastosowanie środków uzupełniających. Należy w tym miejscu zaznaczyć, że do instrumentów tych zalicza się środki umowne, techniczne oraz organizacyjne. Środki umowne obejmują jednostronne zobowiązania albo kontakty dwu- lub wielostronne zawierane pomiędzy podmiotem, który przekazuje dane a podmiotem, który je odbiera. Należy zaznaczyć, że nie są one traktowane jako umowy międzynarodowe w rozumieniu norm prawa międzynarodowego publicznego. Wśród środków o charakterze technicznym można wskazać natomiast takie instrumenty, jak: wykorzystanie algorytmu i protokołu szyfrowania, pseudonimizacja danych, przetwarzanie dzielone czy



przetwarzanie przez wiele podmiotów. Do środków organizacyjnych zaliczyć należy z kolei określone polityki wewnętrzne i standardy stosowane przez administratorów danych osobowych, podmioty przetwarzające oraz podmioty odbierające dane w państwach trzecich. W ramach takich praktyk można wyodrębnić np. obowiązek zachowania w tajemnicy danych osobowych przez pracowników zatrudnionych przy ich przetwarzaniu czy tzw. „politykę czystego biurka".

Przyjęcie takich środków może okazać się krokiem niezbędnym dla zapewnienia odpowiedniego stopnia ochrony danych osobowych przekazywanych do państwa trzeciego. Ich wybór w każdym przypadku następuje indywidualnie, w zależności od operacji przekazywania danych i stosowanych narzędzi zabezpieczenia. Najbardziej efektywne jest połączenie kilku rodzajów środków, dzięki czemu uzyskuje się wyższy poziom ochrony danych osobowych.

POROZUMIENIE DOTYCZĄCE TRANSFERU DANYCH

Z perspektywy stosunków pomiędzy Unią Europejską a Stanami Zjednoczonymi warto postulować de lege ferenda, aby doszło do wypracowania wzajemnego porozumienia, na mocy którego będzie możliwe stwierdzenie odpowiedniego poziomu ochrony danych osobowych i wprowadzenie podstawy transferu danych, podobnej do uchylonej już Tarczy Prywatności. Niewątpliwie pomogłoby to w ujednoliceniu procedury przekazywania danych osobowych do Stanów Zjednoczonych i ułatwiłoby ją.

Etapy zapewnienia zgodności z unijnym poziomem ochrony danych osobowych są obecnie związane z koniecznością spełnienia określonych przesłanek i bieżącego monitorowania sytuacji prawnej w państwie trzecim, do którego przekazywane są dane. Zdecydowanie negatywnie przedstawia się również brak możliwości oparcia działania związanego z ochroną danych na kodeksach postępowania - te bowiem muszą być zatwierdzone, a dotychczas w Polsce nie wydano żadnej decyzji w tym zakresie.

Znaczenie wyroku Schrems II dla transferu danych osobowych

Wprowadzenie instrumentu, na mocy którego możliwe byłoby przekazywanie danych osobowych z Unii Europejskiej do Stanów Zjednoczonych bez konieczności stosowania dodatkowych zabezpieczeń byłoby zatem zdecydowanie pożądane. Nie wiadomo jednak, czy i kiedy dojdzie do wypracowania porozumienia, które umożliwiłoby współpracę w tym zakresie, jednocześnie zapewniając bezpieczeństwo danych osobowych obywateli Unii Europejskiej.

ZOSTAŃ EKSPERTEM

SECURITY MAGAZINE

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

REDAKCJA@SECURITYMAGAZINE.PL

EDUKACJA KLUCZEM DO POPRAWY CYBERBEZPIE-CZEŃSTWA W FIRMIE

Maciej Pawlak
Tpay

“Bądź zmianą, którą chcesz ujrzeć w świecie” – czy ta mądrość Mahatma Gandhiego jest zbyt podniosła, by używać jej w kontekście cyberbezpie-czeństwa? Biorąc pod uwagę, jak ogromną rolę odgrywa tu edukacja pracowników oraz przewidywanie przyszłości, jestem przekonany, że jest wręcz drogowskazem.

Przestrzeń internetowa daje przestępcom ogromne pole do działania. Ryzyko stania się ofiarą cyberprzestępstwa z każdym rokiem wzrasta. Okres pandemii był wyjątkowy pod względem liczby oszustw w sieci. Według danych rynkowych, w ubiegłym roku w Polsce 69 proc. firm odnotowało przynajmniej jeden cyberatak. Problem ten dotyczy jednak nie tylko instytucji. Na przykład, z szacunków Rzecznika Finansowego, powstałych w oparciu o dane Narodowego Banku Polskiego, wynika, że w 2021 roku mogło dojść do 250 tys. przestępstw polegających na utracie dużych środków finansowych przez nieautoryzowane transakcje.

Zwiększenie skali działalności cyberprzestępców ma dwojakie przyczyny. Po pierwsze, sprzyja im przeniesienie wielu naszych aktywności do sieci, panująca pandemia oraz praca zdalna. Po drugie, rozwój technologii i digitalizacja sprawiają, że w internecie można znacznie łatwiej okradać większą liczbę osób.

Mimo że większość z nas korzysta na co dzień z innowacji i załatwia wiele spraw przez internet, to świadomość na temat wiążących się z tym zagrożeń, wciąż jest relatywnie mała, także wśród firm.

OBECNE WYZWANIA

Jednym z najpopularniejszych ataków w cyberprzestrzeni jest **phishing**, który polega na wykorzystywaniu wiadomości mailowych lub SMS-ów. Według raportu NASK z 2021 roku, to właśnie ta metoda stanowiła najczęstszy rodzaj cyberataków i dotyczyła aż 73 proc. wszystkich zgłaszanych incydentów.

Do niedawna sporą nowością była informacja, że oszuści wysyłają wiadomości zawierające linki kierujące do fałszywych stron np. banków. Dziś działania cyberprzestępców są znacznie bardziej zaawansowane i wyrafinowane.

Coraz częściej przed atakiem oszuści dokładnie i długo obserwują ofiarę, którą może być zarówno osoba prywatna, jak i przedstawiciel instytucji. To tzw. **ataki APT** (Advanced Persistent Threat), czyli celowane. Przestępcy internetowi wykorzystują nasze przyzwyczajenia i rutynę, by naj-pierw wykraść dane osobowe, a następnie środki z konta bankowego, cenne dane czy tajemnicę przedsiębiorstwa.

Niezwykle ważna jest więc czujność, a co z tym idzie, szeroko zakrojona edukacja. Im więcej wiemy na temat działań cyberprzestępców, potrafimy się przed nimi chronić i efektywnie reagować, gdy jednak dojdzie do ataku, tym większe szanse na uchronienie się przed stratami lub ich zmniejszenie. Wśród szefów największych światowych organizacji aż 80% wie, że cyberataki są jednym z największych zagrożeń dla rozwoju biznesu. Jednocześnie jednak firmy deklarują, że na cyberbezpieczeństwo przeznaczają średnio zaledwie 3 proc. swojego całkowitego budżetu IT.

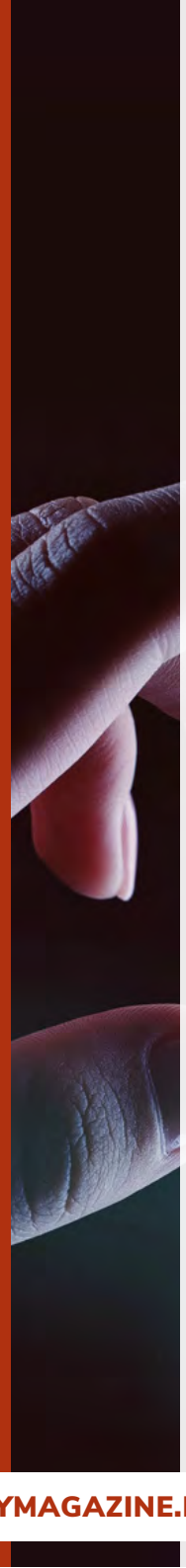
ZAPOBIEGAJ ATAKOM LUB ICH SKUTKOM

- **Przygotuj strategię bezpieczeństwa i dostosuj ją do zmieniających się warunków, tj. ewolucji metod działań cyberprzestępców.**
- Dopilnuj, by treść strategii była jasna dla pracowników – nie spełni ona swojej roli, jeśli zespół nie będzie jej rozumiał i potrafił wykorzystywać.
- **Pamiętaj, że cyberataki mogą dotknąć każdą osobę, bez względu na jej stanowisko czy staż pracy.**
- Uczulaj zespół na kwestie związane z cyberbezpieczeństwem. Jeśli jesteś w firmie specjalistą od tych zagadnień, pamiętaj o tzw. klątwie wiedzy – nie wszystko, co jest dla ciebie jasne, wiedzą pozostali członkowie zespołu.
- **Edukuj, organizuj szkolenia, dziel się wiedzą.**
- Zabezpiecz kanały komunikacji w firmie i przypominaj pracownikom, aby o sprawach firmowych rozmawiali lub pisali tylko na kanałach służbowych.
- **Ułatw zespołowi zgłaszanie potencjalnych ryzyk lub ataków, możesz w tym celu udostępnić odpowiednie narzędzie czy szablon.**
- W przypadku ataku, zadbaj o działanie zgodnie z procedurą i w zależności od sytuacji, odpowiednio informuj zespół lub grupy pracowników.
- **Wyciągaj wnioski z trudnych sytuacji, które was dotknęły.**
- Bądź na bieżąco z informacjami publikowanymi w internecie, jeśli pracownik czy firma stała się ofiarą – mogą mieć one wpływ na wizerunek marki i dalsze bezpieczeństwo.
- **Korzystaj z najlepszych rozwiązań i narzędzi, które pomagają dbać o bezpieczeństwo – skutki ataku mogą być znacznie bardziej dotkliwe finansowo, niż inwestycja w opcje zabezpieczające.**

Jeśli prowadzisz firmę, której klienci np. podczas korzystania z twoich usług, mogą stać się ofiarami cyberprzestępcy, pamiętaj o ich edukowaniu i supportowaniu oraz o odpowiedniej transparentności – nawet, jeśli po twojej stronie wszystko zostało odpowiednio zabezpieczone.

Do wyższej skuteczności cyberprzestępców przyczynia się rosnąca obecnie **automatyzacja**, która znacznie przyspiesza działania oszustów. Cyberprzestępcy najpierw starają się jak najdokładniej poznać firmę i jej strukturę, wykorzystują do tego np. serwis LinkedIn lub inne informacje dostępne w internecie. Dysponują narzędziami, które pobierają informacje na temat firmy, zbierają dane osobowe uwzględniające stanowiska i zakresy obowiązków pracowników. Następnie nawiązują kontakt z potencjalną ofiarą poprzez przybranie cudzej tożsamości, inicjują rozmowę, która prowadzi np. do dobrowolnego (nieświadomego) przekazania środków finansowych przez oszukaną osobę. Na przykład pracownik działu kadr otrzymuje maila od współpracownika, w którym prosi on o zmianę numeru swojego konta bankowego, po to, by najbliższa wypłata znalazła się już na nowym. Wiadomość bardzo przypomina taką, jaką zwykle wysyłają pracownicy danej firmy. Jeśli odbiorca wiadomości nie będzie dostatecznie czujny, środki trafią na konto przestępcy.

Warto pamiętać, że cyberprzestępcy mają dostęp do tych samych narzędzi, co my, ale mogą ich używać w innym kontekście.



Coraz bardziej popularnym działaniem jest wykorzystywanie botów. Zapewne już większość z nas spotkała się z sytuacją, że dzwoni do nas nieznany numer, okazuje się, że jest to przedstawiciel firmy i chce przedstawić ofertę, a nam trudno jest odróżnić, czy po drugiej stronie słuchawki jest człowiek, czy maszyna.

PRZYSZŁOŚĆ

W sprawie cyberprzestępczości naprawdę trudno określić, jakie działanie jest już rzeczywistością, a jakie czeka nas w przyszłości. Dobrym przykładem jest **deepfake** (ang. deep learning, – głębokie uczenie + fake – fałszywy), czyli obróbka obrazu polegająca na łączeniu obrazów ludzkich twarzy przy użyciu technik sztucznej inteligencji. Tworzone są w ten sposób filmy, nagrania audio czy zdjęcia. Biorąc pod uwagę wspomniane boty, już nietrudno wyobrazić sobie sytuację, że z pracownikiem kontaktuje się efekt komputerowej obróbki, zamiast prawdziwego człowieka. Nie jest to jeszcze zbyt częsta technika wykorzystywana przez oszustów, ale deepfake to narzędzie, które może stać się nowym zagrożeniem w cyberprzestrzeni.

W 2018 roku media społecznościowe obiegło nagranie postaci łudząco przypominającej Baracka Obamę, tłumaczącej, aby nie wierzyć we wszystko, co widzi się w internecie. Obecnie tworzenie tego typu filmów wykorzystywane jest głównie przeciwko osobom sławnym lub w celu kreowania humorystycznych nagrań.

Tego typu zjawisko trzeba jednak potraktować jako przestrogę – filmy mogą być w przyszłości wykorzystywane w celach informacyjnych. Jak bardzo daleka jest to przyszłość?

Nie ma idealnego rozwiązania, które zapobiega cyberprzestępczości. Wiemy jednak, co się sprawdza najlepiej – edukacja. Uświadamianie, odpowiadanie na pytania i udostępnianie odpowiednich narzędzi, to znacznie lepsza droga, niż wyłącznie pociąganie pracowników do odpowiedzialności. Zaniedbywanie tych działań prowadzi do ukrywania przez członków zespołu ataków lub nieposiadania przez nich umiejętności identyfikowania podejrzanych sytuacji. W dobie tak szybkiego rozwoju cyberprzestępczości, żadnej firmy na to nie stać.

JAK WYKRYĆ DEEPFAKE?

- Sprawdź, czy dźwięk zgrywa się dokładnie z ruchem ust. Zdarzają się sytuacje, w których ruch ust osoby na filmie jest nieco spowolniony, bądź całkowicie nie pasuje do dźwięku.
- Zwróć uwagę na szczegóły, np. kolor skóry, ułożenie głowy w stosunku do reszty ciała, refleksy świetlne na przedmiotach, odbicia światła w biżuterii czy na zębach.
- Sprawdź, czy nagranie audio i wideo jest podobnej jakości (za-zwyczaj ścieżka audio jest gor-szej jakości).
- Upewnij się, że osoba występująca na nagraniu mruga powiekami.

tpay zaufane płatności

www.tpay.com

SECURITYMAGAZINE.PL

BEZPIECZEŃSTWO FIRMOWEGO ROUTERA

Redakcja
SECURITY MAGAZINE

Routery nierzadko padają ofiarami cyberprzestępców. Tak – router można zhakować i może mieć to niezwykle poważne konsekwencje. Dość powiedzieć, że w 2022 roku jeden pentester zdołał wyłączyć cały internet w Korei Północnej właśnie dzięki atakowi na router. Na co powinieneś zwrócić uwagę w kwestii routerów w swojej firmie?

AMERYKAŃSKI PENTESTER KONTRA KOREA PÓŁNOCNA

W 2021 r. amerykański niezależny specjalista od cyberbezpieczeństwa ukrywający się pod pseudonimem P4x został zaatakowany przez północnokoreańską grupę hakerów sponsorowaną przez reżim. Amerykaninowi udało się odeprzeć ich atak i powstrzymać przed wykradnięciem jakichkolwiek wartościowych rzeczy. Nie był jednak zadowolony z tego, że stał się ofiarą ataku, a także że rząd amerykański nic z tym nie zrobił. Sam zatem postanowił wymierzyć sprawiedliwość.

Przez rok P4x przygotowywał się do odwetu i w końcu zaatakował północnokoreańskie syste-my. Udało mu się znaleźć liczne luki i błędy, co pozwoliło mu dokonać cyberataków na tzw. kry-tyczne routery i serwery reżimu. Dzięki temu praktycznie odciął cały kraj od lokalnego inter-netu, blokując najważniejsze strony Korei Pół-nocnej.

W tym m.in. osobistą stronę Kim Dzong Una, czy tamtejszych linii lotniczych. Północni Koreańczycy mogli łączyć się tylko z zagranicznymi serwisami lub ich własnymi witrynami, które posiadały serwery za granicą, np. Uriminzokkiri.com.

Jednak ponieważ cyberataki P4x wymierzone były głównie w tamtejsze routery, to dosłownie niemożliwe byłoby skierowanie danych do Korei Północnej. W praktyce takie ataki mogą doprowadzić nie tylko do zakłócenia działania stron internetowych, ale też np. poczty e-mail. Czego uczy nas ta historia? Że routery, to potencjalne słabe ogniwa, które mogą zostać wykorzystane przez hakerów.

ZWIĘKSZA SIĘ LICZBA LUK W ROUTERACH

Od momentu wybuchu pandemii koronawirusa cyberbezpieczeństwo routerów stało się niezwykle ważne, a one same są zagrożone jak nigdy dotąd. Bardziej świadomi użytkownicy internetu czy też firmy, wiedzą, jak ważną część infrastruktury stanowią te „małe, świecące skrzyneczki". To de facto brama do internetu w Twoim domu czy biurze.

Router jest właściwie praktycznie osobnym, pełnoprawnym komputerem z własnym systemem operacyjnym.

Poprzez zhakowanie routera cyberprzestępca uzyska możliwość zakłócania jego pracy (a w konsekwencji całej sieci w danym miejscu), czy szpiegowania użytkowników. Dzięki atakom ty-pu „man-in-the-middle" haker może zmieniać niezaszyfrowane dane, kierować użytkowników do tzw. złych bliźniaków (czyli stron podszywających się pod inne), przejąć maile czy uzyskać dostęp do bankowości internetowej.

Według danych serwisu cve.mitre.org liczba luk w zabezpieczeniach routerów w latach 2011–2021 wzrosła z 26 do 321. W samych tylko latach 2020–2021 wykryto ponad 500 luk w routerach. To one pozwalają hakerom uzyskiwać do nich dostęp. A niestety – producenci routerów równie często nie dbają o ich bezpieczeństwo, co sami użytkownicy.

Michael Horowitz podczas konferencji HOPE X w Nowym Jorku wskazał, że wiele domowych rou-terów klasy konsumenckiej nie powiadamia użytkowników, jeśli i kiedy dostępne są aktualizacje ich oprogramowania. Choć jak podkreślał – te są niezbędne do załatania luk w zabezpieczeniach. Horowitz dosłownie przestrzegał uczestników konferencji, aby nie kupowali popularnych, tanich routerów w sieciach sklepów RTV AGD.

Twierdził też, że nie powinniśmy używać routerów przekazywanych przez dostawców usług multimedialnych. Dlaczego? Bo jest ich miliony i są w zasadzie takie same, a przez to cyberprzestępcom łatwiej jest znaleźć w nich luki.

JAK HAKERZY WYKORZYSTUJĄ LUKI W ROUTERACH?

Słabe punkty w routerach umożliwiają cyberprzestępcom ominięcie funkcji ochrony hasłami (takie jak np. ograniczenie prób logowania czy zabezpieczenie CAPTCHA), ominięcie uwierzytelniania, wysyłanie zdalnych poleceń do routerów, a nawet wyłączania ich. Najprostsze do zhakowania są właśnie routery w klasie konsumenckiej, czyli te najtańsze lub masowo dostarczane przez operatorów usług multimedialnych.

Zdarza się też (i to nierzadko), że hakerzy wykorzystują przejęte routery (i urządzenia IoT) do tworzenia botnetów, czyli sieci zainfekowanych maszyn pozwalających m.in. na masowe rozsyłanie spamu lub ataki DDoS. Najpopularniejszym takim botnetem jest Mirai, który składa się głównie z routerów, czy inteligentnych kamer. Co ciekawe – początkowo służył do przeprowadzania ataków DDoS na serwery Minecrafta.

Problem routerów jako słabego ogniwa stanowi przede wszystkim wykorzystywanie przestarzałych zabezpieczeń. Mowa tu chociażby o Home Network Administration Protocol (HNAP), które przesyła poufne informacje o routerze przez internet pod adresem http://[adres IP routera]/HNAP1/.

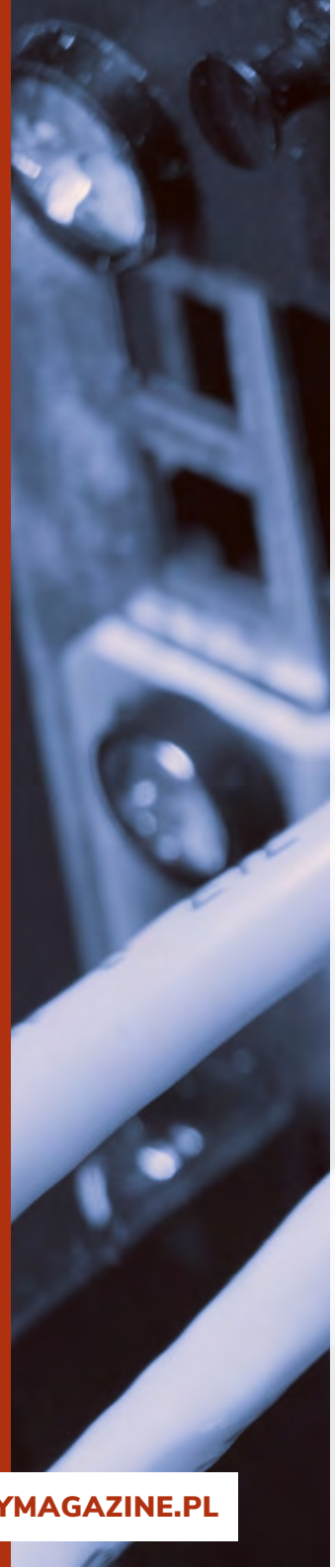
W 2014 r. HNAP znalazł się na ustach całej branży cyberbezpieczeństwa, kiedy to robak The Moon wykorzystał ów protokół do zidentyfikowania podatnych na ataki routerów marki Linksys. Firma szybko zaktualizowała swoje systemy, co pozwoliło na zabezpieczenie się przed takimi atakami, ale niesmak pozostał.

Od tamtej pory HNAP pojawia się coraz rzadziej, ale często nadal jest wykorzystywany przez starsze routery. A przecież te nie wymieniamy tak często. Większość z nas w zasadzie robi to tylko, kiedy zmienia usługodawcę lub gdy ten sam dostarczy nam nowy router, bo stary uległ awarii albo jest przestarzały.

Problem poniekąd stanowi też Universal Plug and Play (UPnP), który zaprojektowano z przeznaczeniem dla sieci LAN. Protokół ten w zasadzie nie ma żadnych zabezpieczeń, przez co do routera można podłączyć praktycznie wszystko.

Inną funkcją, która naraża Twój router na potencjalne przejęcie go jest tzw. Wi-Fi Protected Setup (WPS). Z pozoru jest ona bardzo wygodna dla użytkownika. Za pomocą ośmiocyfrowego PIN-u pozwala na ominięcie hasła sieciowego i podłączenia urządzeń do sieci Wi-Fi. To faktycznie może być przydatne, gdy np. zapomnimy hasła do WiFi (choć te powinniśmy trzymać np. w zabezpieczonych menedżerach haseł). De facto są to jednak „tylne drzwi", przez które niejeden haker dostaje się do „naszego domu".

PIN ten najczęściej był zamieszczany z tyłu routera, a zatem wystarczy, tylko aby ktoś wszedł



do naszego biura, zrobił zdjęcie i już uzyskuje dostęp do całej sieci Wi-Fi. A czasem nawet nie musi fizycznie pojawiać się w biurze.

W końcu hakerzy często wykorzystują socjotechniki, szantażując lub wpływając na pracowników, aby wyłudzić od nich konkretne hasła, dane czy dostępy. Co najgorsze, jak wskazuje Michael Horowitz – zazwyczaj wspomniane 8-cyfrowe PIN-y nawet nie są... 8-cyfrowe. 8. cyfrą najczęściej jest suma pozostałych 7. Co za tym idzie cyberprzestępca ma ok. 11 tys. możliwych kodów do odgadnięcia (a ten proces można zautomatyzować), aby przejąć Twój router.

JAK ZABEZPIECZYĆ SWÓJ ROUTER PRZED CYBER-PRZESTĘPCAMI?

Pierwszą i podstawową rzeczą w kwestii cyberbezpieczeństwa routerów jest **rozdzielenie ich od modemów**. Bardzo często producenci czy operatorzy usług internetowych dostarczają swoim klientom tylko sam router. Główna różnica polega na tym, że **router nie odbiera internetu, a rozdziela sygnał pomiędzy urządzenia w prywatnej sieci i nadaje każdemu z osobna adres IP. Umożliwia to tworzenie sieci lokalnej.**

Modem z kolei moduluje sygnał z zewnątrz – od dostawcy – na informację cyfrową, by następnie ją demodulować. Dzięki modemowi można odbierać sygnał internetu na dowolnym urządzeniu znajdującym się w zasięgu. Modem może być podłączony na raz tylko do jednego urządzenia, np. komputera stacjonarnego. Z kolei z routera korzysta wiele urządzeń w tym samym czasie, ale oddzielnie (własne adresy IP, sieć lokalna).

Drugą sprawą jest niekorzystanie ze zwykłych, konsumenckich routerów. Te naprawdę często mają bardzo słabe zabezpieczenia, luki i są rzadko aktualizowane.

Jeśli zależy Ci na cyberbezpieczeństwie, powinieneś używać komercyjnego routera lepszej klasy. Kosztują one przeważnie zaledwie kilkaset złotych, a mogą sprawić znacznie większe trudności hakerom niż standardowe modele dostarczane przez operatorów. Komercyjne routery lepszej klasy nie korzystają z UPnP czy WPS, co już podnosi ich bezpieczeństwo.

Musisz też zadbać także o hasło do sieci internetowej w biurze. Nie powinno być ono krótsze niż 16 znaków – to dzisiejszy minimalny standard. I tu ponownie pojawia się kwestia routerów konsumenckich, bo te nierzadko nie przyjmują haseł o takiej długości. Nie mówiąc już o dłuższych. Nie warto zostawiać domyślnych haseł i zabezpieczeń. I choć to oczywiste, to niestety nie jest to standard. Jak pokazuje badanie firmy Bro-adband Genie, 48% respondentów nie zmieniło żadnego z ustawień swojego routera – w tym domyślnego hasła. 73% dlatego, że nie widzi ta-kiej potrzeby, a kolejne 20%, ponieważ nie wie, jak to zrobić.

To tyle z podstawowych zabezpieczeń.

Warto jednak też:

- Włączyć szyfrowanie bezprzewodowe WPA2 lub WPA3, aby nieautoryzowani użytkownicy nie mogli korzystać z sieci internetowej. Jeśli Twój router nie obsługuje tych szyfrowań, a jedynie np. WEP – czas go zmienić;
- Włączyć automatycznie aktualizowanie routera;
- Skonfigurować sieć Wi-Fi dla gości tak, aby wyłączała się automatycznie po określonym czasie;
- Połącz urządzenia typu IoT do sieci dla gości, a nie podstawowej, co pozwoli zminimalizować szkody z potencjalnego cyberataku;
- Wyłączaj zdalny dostęp do routera, kiedy tego nie potrzebujesz. Albo całkowicie go dezaktywuj;
- Zmień domyślną nazwę sieci Wi-Fi dla Twojego biura, aby uniemożliwić jej identyfikacje osobom z zewnątrz;
- Jeśli to możliwe, a Twoje urządzenia są z tym kompatybilne – ustaw router na pasmo 5 GHz, zamiast 2,4 GHz;
- Jeśli to możliwe – wyłącz dostęp administracyjny przez Wi-Fi. Administratorzy po-

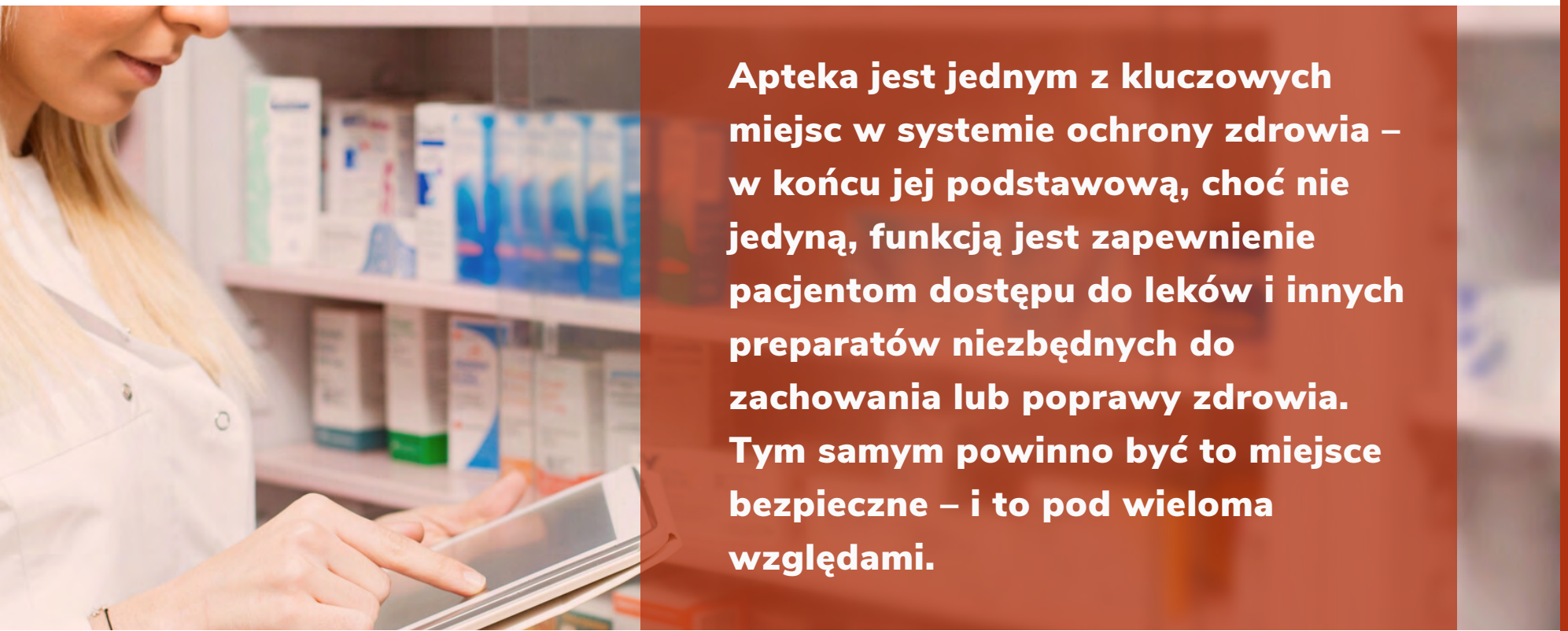
winni powinni łączyć się z routerami tylko poprzez sieć Ethernet;

- Jeśli to możliwe – korzystaj z VPN-ów, trybu incognito lub przeglądarek czy wyszukiwarek nastawionych znacznie bardziej na prywatność;
- Włącz opcję nieodpowiadania na polecenie PING w swoim routerze.

Wdrożenie tych rozwiązań do Twojej firmy, zdecydowanie pozytywnie wpłynie na jej cyberbezpieczeństwo i ograniczy szansę przejęcia routera przez hakera.

CZY W APTEKACH BĘDZIE BEZPIECZNIEJ?

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



Apteka jest jednym z kluczowych miejsc w systemie ochrony zdrowia – w końcu jej podstawową, choć nie jedyną, funkcją jest zapewnienie pacjentom dostępu do leków i innych preparatów niezbędnych do zachowania lub poprawy zdrowia. Tym samym powinno być to miejsce bezpieczne – i to pod wieloma względami.

Zapewnienie bezpieczeństwa danych pacjentów (zwłaszcza przed możliwością zapoznania się z nimi przez osoby postronne) oraz ich bezpieczeństwa zdrowotnego (przede wszystkim poprzez wdrożenie odpowiednich rozwiązań sanitarnych – w końcu w aptece bardzo często znajdują się osoby chore) to najważniejsze z wyzwań, jakie stoją przed prowadzącymi apteki. Jednak nie mniejszym wyzwaniem jest obecnie zapewnienie bezpieczeństwa także pracownikom aptek, w tym zwłaszcza farmaceutom i technikom farmaceutycznym. Nieraz w aptekach pojawiają się osoby agresywne, żądające np. bezprawnego wydania środków psychoaktywnych. Tymczasem niedawno prawne aspekty zabezpieczenia bezpieczeństwa farmaceutów i techników farmaceutycznych znacznie się poprawiły. Co to oznacza w praktyce?

APTEKARZ FUNKCJONARIUSZEM PUBLICZNYM

W drugiej połowie czerwca – po złożeniu podpisu przez prezydenta – zakończył się proces legislacyjny noweli Prawa farmaceutycznego, na mocy której farmaceucie oraz technikowi farmaceutycznemu ustawodawca przyznał status funkcjonariusza publicznego. Bez wątpienia jest to znaczna nobilitacja tych zawodów, jednak istotą nowych rozwiązań prawnych – na co wskażę uwagę szerzej poniżej – nie jest podnoszenie ich prestiżu, ale zwiększenie poziomu bezpieczeństwa aptekarzy. Otóż zmiany te – o które od dawna zabiegały środowiska farmaceutyczne – stanowią reakcję na coraz częściej zdarzające się ataki na pracowników aptek.

Zgodnie z obowiązującym od 12 lipca br. art. 35a ustawy o zawodzie farmaceuty, farmaceuta podczas i w związku z wykonywaniem w aptece ogólnodostępnej lub punkcie aptecznym ściśle wskazanych czynności, korzysta z ochrony przewidzianej dla funkcjonariusza publicznego na zasadach określonych w ustawie z dnia 6 czerwca 1997 r. – Kodeks karny. Czynności te to: sprawowanie opieki farmaceutycznej oraz udzielanie usług farmaceutycznych w zakresie wydawania z apteki lub punktu aptecznego produktów leczniczych; przeprowadzania wywiadu farmaceutycznego; udzielania porady farmaceutycznej w celu zapewnienia prawidłowego stosowania produktu leczniczego, wyrobu medycznego lub środka spożywczego specjalnego przeznaczenia żywieniowego; wykonywania pomiaru ciśnienia krwi. Analogiczne rozwiązania zawarto w ustawie – Prawo farmaceutyczne w stosunku do techników farmaceutycznych.

W tym kontekście trzeba pamiętać, że farmaceucie (magistrowi farmacji) oraz technikowi farmacji ochrona właściwa dla funkcjonariuszy publicznych nie przysługuje w każdej sytuacji, ale tylko „podczas i w związku z wykonywaniem w aptece ogólnodostępnej lub punkcie aptecznym" wymienionych powyżej czynności. Nie chodzi tu jednak tylko i wyłącznie o sytuacje, w których aptekarz będzie realizował swoje obowiązki w czasie godzin pracy w aptece ogólnodostępnej/punkcie aptecznym – nawiasem mówiąc apteki szpitalne w ogóle zostały wyłączone spod zakresu tej regulacji. „Podczas i w związku" obejmuje wszystkie zdarzenia godzące w aptekarza, a mające związek z jego pracą. Może się okazać, że np. zostanie on zaatakowany przez napastnika, któremu nie wydał żądanego przez niego preparatu już po opuszczeniu apteki. Każdą więc taką sytuację trzeba będzie oceniać osobno.

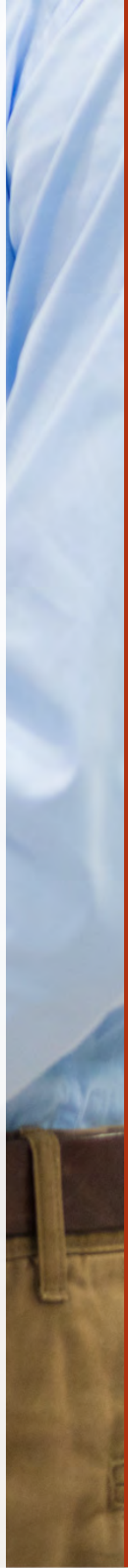
KIM JEST FUNKCJONARIUSZ PUBLICZNY?

Analizy te będą uskuteczniać się przede wszystkim na gruncie procedury karnej. Wynika to z faktu, że przyznanie komukolwiek statusu funkcjonariusza publicznego – a warto pamiętać, że status ten przysługuje chociażby posłom, senatorom, sędziom, prokuratorom czy komornik – ma na celu przede wszystkim zaostrzenie od-

powiedzialności karnej za popełnienie przestępstw godzących w dobra prawne takich osób, zwłaszcza ich nietykalność cielesną, czy mówiąc szerzej, bezpieczeństwo. Aby udowodnić tę tezę wystarczy – nawet pobieżny – rzut oka na przepisy Kodeksu karnego.

Zgodnie z art. 222 § 1 Kodeksu karnego **kto narusza nietykalność cielesną funkcjonariusza publicznego podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat trzech. Tymczasem naruszenie nietykalności cielesnej osób nieposiadających tego statusu jest zagrożone maksymalną karą do roku więzienia (art. 217 § 1 k.k.), a w przypadku, gdy przestępstwo to popełniono w związku z podjętą przez daną osobę interwencją na rzecz ochrony bezpieczeństwa ludzi lub ochrony bezpieczeństwa lub porządku publicznego, do dwóch lat pozbawienia wolności (art. 217a k.k.)**. Jeszcze czytelniejszym przykładem jest zakres zagrożenia karą za zabójstwo funkcjonariusza publicznego. Sprawca takiego czynu podlega karze więzienia na czas nie krótszy, niż 12 lat (art. 148 § 3 k.k.).

Z surową odpowiedzialnością karną muszą liczyć się sprawcy takich przestępstw, jak czynna napaść na funkcjonariusza publicznego (art. 223 k.k.), zastosowanie wobec niego wymuszenia (art. 224 § 2 k.k.) czy znieważenia (art. 226 k.k.)



CZY RZECZYWIŚCIE COŚ SIĘ ZMIENI?

Regulacje prawne nigdy nie działają same przez się – zawsze trzeba je odpowiednio zastosować. Dlatego, jeżeli nieodpowiednie zachowania skierowane przeciwko aptekarzom nie spotkają się z odpowiednią reakcją organów ścigania, to nowe przepisy pozostają martwą literą prawa. Właściwie jedynym ich oddziaływaniem może być wpływ na społeczeństwo w zakresie prewencji generalnej, a więc – mówiąc najogólniej – odstraszanie, poprzez surowość grożącej kary, potencjalnych sprawców przestępstw przeciwko farmaceutom i technikom farmaceutycznym od ich popełnienia. Jednak wa-runkiem tego rodzaju oddziaływania również jest prawidłowe stosowanie sankcji karnych, a więc ich nieuchronność dla każdego sprawcy przestępstwa.

Dlatego to, czy faktycznie w aptekach będzie bezpieczniej, a jednocześnie wzrośnie poziom bezpieczeństwa samych aptekarzy, zależy od wielu czynników. Zwłaszcza zaś od tego, w jaki sposób organy ścigania wykorzystają nowe rozwiązania legislacyjne, a farmaceuci i technicy farmaceutyczni zaangażują się w ochronę swoich praw. Z kolei do takiej aktywności warto nieustannie zachęcać przedstawicieli wszystkich zawodów medycznych.

TO, CZY FAKTYCZNIE W APTEKACH BĘDZIE BEZPIECZNIEJ, A JEDNOCZEŚNIE WZROŚNIE POZIOM BEZPIECZEŃSTWA SAMYCH APTEKARZY, ZALEŻY OD WIELU CZYNNIKÓW. ZWŁASZCZA ZAŚ OD TEGO, W JAKI SPOSÓB ORGANY ŚCIGANIA WYKORZYSTAJĄ NOWE ROZWIĄZANIA LEGISLACYJNE, A FARMACEUCI I TECHNICY FARMACEUTYCZNI ZAANGAŻUJĄ SIĘ W OCHRONĘ SWOICH PRAW.


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

EKSPERCI WYDANIA

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

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

SIER. PAWEŁ ŁADNA
Cyber Security Specialist

Były funkcjonariusz pionu kryminalnego Komendy Stołecznej Policji, zajmujący się zwalczaniem przestępczości elektronicznej. Posiadający doświadczenie cywilne z zakresu zgodności cyberbezpieczeństwa i konsultant w zakresie tworzenia i wdrażania strategii cyberbezpieczeństwa w międzynarodowej firmie konsultingowej. Na co dzień oddany rodzinie, biegacz-amator i miłośnik gór, wycieczek i biwaków.

JACEK MRZYGŁÓD
Employer Branding and
Communications Lead
Evolution Poland

Od lat zajmuje się zawodowo employer brandingiem oraz employee experience. Pracował naukowo na SGH, w agencji badawczej, potem w amerykańskiej firmie konsultingowej na Bliskim Wschodzie. Głęboko wierzy, że da pogodzić się cele biznesowe firm z dbałością o pracowników. Szczęśliwy ojciec, pasjonat piłki nożnej oraz książek na temat utopii i dystopii.

WOJCIECH ŚWIĄTEK
Cybersecurity Senior Analyst
EY

Starszy analityk w zakresie przeglądów bezpieczeństwa infrastruktury IT oraz oceny ryzyka utraty poufności, integralności i dostępności w tym obszarze.

EKSPERCI WYDANIA

ŁUKASZ TOCZEK
Serwisant systemów aptecznych
MERIDO

Pasjonat nowinek technologicznych, zahartowany przez Windows 95. Wyzwania zawodowe traktuje jako nieodłączną część pracy. W wolnych chwilach wędruje i odkrywa uroki miejsc nieoczywistych. Gdy pogoda nie sprzyja, podróżuje w świecie wyobraźni przy kolejnej lekturze.

MACIEJ PAWLAK
Head of Risk & Security
Tpay

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

DARIUSZ TWORZYDŁO
Prezes
EXACTO

Ekspert z zakresu PR, doradza zarządom firm, jest trenerem i konsultantem. Wykonuje ekspertyzy, analizy komunikacji wewnętrznej. Opracowuje strategie PR i marketingu. Profesor Uniwersytetu Warszawskiego. Prezes spółki Exacto. Prezes zarządu Stowarzyszenia Agencji Public Relations. Autor ponad 270 artykułów naukowych i publicystycznych, prac badawczych i książek.

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

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

PARTNERZY WYDANIA

POLITYKA BEZPIECZEŃSTWA

SERWIS INFORMACYJNY
O BEZPIECZEŃSTWIE FIRM

RZETELNY REGULAMIN

BLOG POŚWIĘCONY
POLSKIEMU E-COMMERCE

ROCKET SCIENCE COMMUNICATIONS

AGENCJA PUBLIC RELATIONS

INNERVALUE

AGENCJA PUBLIC RELATIONS

Polityka® Bezpieczeństwa

Rzetelny® Regulamin

Rocket Science Communications

InnerValue investor relations

ZOBACZ WYDANIA

Wydanie 1/2022

POBIERZ

Wydanie 2/2022

POBIERZ

Wydanie 3/2022

POBIERZ

Wydanie 4/2022

POBIERZ

WYDAWCA

Wydawca:

Rzetelna Grupa sp. z o.o.

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

KRS 284065
NIP: 524-261-19-51
REGON: 141022624
Kapitał zakładowy: 50.000 zł
Sąd Rejonowy dla m. st. Warszawy I XIII Wydział Gospodarczy
Magazyn wpisany do sądowego Rejestru dzienników i czasopism.

Redaktor Naczelny: Rafał Stępniewski

Redakcja: Monika Świetlińska, Damian Jemioło
Projekt i skład: Monika Świetlińska

Współpraca i kontakt: redakcja@securitymagazine.pl

SECURITYMAGAZINE.PL