

Rozwój e-usług w rolniczych ubezpieczeniach społecznych – szanse i zagrożenia

Robert Żółtaszek

Abstrakt

Cyfrowa transformacja dla coraz większej części polskiego społeczeństwa musi odbywać się równomiernie we wszystkich grupach społecznych, aby mogła wspierać rozwój naszej gospodarki i być jej siłą napędową. Rozwój e-usług, e-administracji jest nieuniknionym procesem, który powinien być dobrze moderowany przez państwo, a w niektórych obszarach wręcz stymulowany i napędzany. Rozwój kompetencji cyfrowych w grupie społecznej jaką są rolnicy, jest ważny z perspektywy równości w dostępie do nowoczesnych usług, technologii, e-państwa. Odpowiednie zagospodarowanie tej przestrzeni może stanowić dodatkowe koło zamachowe naszej gospodarki, być jej wspomagającym silnikiem wyznaczającym nowe poziomy konkurencyjności. Od 2015 roku w procesie tym aktywnie uczestniczy Kasa Rolniczego Ubezpieczenia Społecznego (KRUS), tworząc i cały czas rozwijając platformę eKRUS, umożliwiającą dostęp online do powiększającej się każdego roku liczby usług dotąd świadczonych na rzecz rolników tylko drogą tradycyjną w Placówkach Terenowych. Artykuł ten przedstawia dotychczasowe osiągnięcia w dziedzinie e-administracji, jak również szanse i zagrożenia związane z cyfryzacją usług publicznych. Tylko świadome jednostki, stale rozwijające swoje kompetencje cyfrowe, są w stanie sprawnie i bezpiecznie poruszać się po wirtualnej przestrzeni, która to wręcz pochłania większą część naszego życia.

Celem opracowania jest przedstawienie dostępnych w Polsce usług on-line administracji publicznej, głównie zintegrowanej platformy eKRUS, ze szczególnym naciskiem na stopień wykorzystania jej przez rolników oraz wskazanie czynników hamujących rozwój e-administracji w wyżej wymienionej grupie społecznej oraz dróg ich niwelowania. Artykuł wskazuje na potrzebę wypracowania metod zwiększania e-kompetencji rolników oraz sposobów dotarcia do tej grupy zawodowej z nowymi narzędziami rozwijającymi powyższe umiejętności.

Słowa kluczowe: cyberbezpieczeństwo, e-administracja, eKRUS, e-państwo, profil zaufany, rolnicy.

Robert Żółtaszek, dr, słuchacz studiów podyplomowych „Rolnicze ubezpieczenia społeczne, funkcjonowanie, administracja i aspekty prawne”, kierownik Placówki Terenowej KRUS w Turku, Kasa Rolniczego Ubezpieczenia Społecznego.

Wstęp

W ostatniej dekadzie rozwój cyfrowego społeczeństwa na świecie przyspieszał z roku na rok, a okres pandemii wywołanej wirusem SARS-CoV-2 dał dodatkowe impulsy do dalszego rozwoju e-usługi, e-pracy, e-nauki. Każdego dnia korzystamy z powiększającej się ilości usług dostępnych za pośrednictwem sieci komputerowej (on-line¹). Proces przenoszenia coraz większej części ludzkiego życia do przestrzeni wirtualnej umiejscowionej w Internecie² nie mógł pozostać niezauważony i być dłużej ignorowany przez instytucje państwowe. Wraz z rozwojem usług komercyjnych powoli następował rozwój e-Państwa i e-administracji, a powszechny dostęp online do usług publicznych stał się kluczowy do dalszego rozwoju społeczno-gospodarczego kraju. Można, co więcej – nawet trzeba stwierdzić, że taki rozwój (e-rozwój) oraz jego skala będą stanowić przewagę konkurencyjności społecznej i ekonomicznej w otoczeniu europejskim i światowym. Liczba osób korzystających z e-administracji systematycznie wzrasta z roku na rok. W 2021 roku 47,5% polskiego społeczeństwa korzystało z usług administracji publicznej za pośrednictwem Internetu. Powiększający się odsetek ludności wykorzystującej to narzędzie w załatwianiu spraw urzędowych ma istotne znaczenie nie tylko społeczne, lecz także ekonomiczne. Jak ważny jest to element naszego życia, uświadomił nam czas pandemii i lockdownu, który zakłócił życie wielu Polaków, a wręcz przerwał dostęp do tak oczywistych usług jak szkoła, urząd, lekarz, bank czy poczta. Wraz z rozwojem e-świata, rozwija się również jego ciemna strona, która stanowi wielkie zagrożenie dla nieświadomych jednostek. Choroby to nie tylko domena ludzka, cyfrowy świat również jest pełen infekcji, tylko dotyczą one urządzeń takich jak komputery, telefony, tablety, drukarki, routery itp. W świecie wirtualnym infekcje wywoływane są przez zarazki, które są złośliwym oprogramowaniem (ang. *malware*³). Malware to wielka rodzina szkodliwych programów obejmujących swym spektrum programy, takie jak wirusy, robaki, trojany, adware, auto-dialery czy inne szkodliwe narzędzia. Aby dalej kontynuować szybki rozwój e-społeczeństwa, e-administracji oraz e-państwa konieczna jest ciągła i na większą skalę edukacja społeczeństwa w zakresie bezpiecznego poruszania się w Internecie oraz rozwijanie szeroko pojętych e-kompetencji. Grupą społeczną, która również jest zainteresowana korzystaniem z usług e-państwa są rolnicy. Od 2015 roku czynnie i nieustannie rozwijana

1. Słownik Języka Polskiego, <https://sjp.pwn.pl/slowniki/ONLINE.html>, dostęp 20.04.2022.

2. Wikipedia, <https://pl.wikipedia.org/wiki/Internet>, dostęp 20.04.2022.

3. Serwis Sekurak, <https://sekurak.pl/robak-trojan-wirus-o-co-w-tym-wszystkim-chodzi/>, dostęp 20.04.2022.

jest platforma eKRUS⁴, dająca możliwość dostępu do usług Kasy Rolniczego Ubezpieczenia Społecznego.

Celem opracowania jest przedstawienie dostępnych w Polsce usług on-line administracji publicznej, głównie zintegrowanej platformy eKRUS, ze szczególnym naciskiem na stopień wykorzystania jej przez rolników oraz wskazanie czynników hamujących rozwój e-administracji w ww. grupie społecznej oraz dróg ich niwelowania.

e-Obywatel, e-Państwo

Często słyszy się sformułowania e-społeczeństwo, e-państwo, e-administracja czy e-usługi. Wszystkie takie sformułowania, tj. z przedrostkiem *e-*, świadczą o istnieniu równoległego świata – świata on-line z nieograniczonym zasobem i możliwościami. Nie ma już znaczenia odległość, godziny dostępu, wszystko jest otwarte 24 godziny na dobę przez siedem dni w tygodniu z każdego miejsca w Polsce i na świecie, z jakiegokolwiek urzędu z dostępem do Internetu. Internet zrewolucjonizował przepływ informacji i dostęp do usług komercyjnych, a przez to również każde państwo, dostęp do urzędów czy informacji publicznej. Państwo Polskie na przykład rozwija i powiększa gamę usług publicznych dostępnych z wykorzystaniem nowych technologii informacyjno-komunikacyjnych (ang. *Information and Communications Technology*, ICT), które wcześniej były świadczone tylko tradycyjnie. Główny Urząd Statystyczny definiuje pojęcie e-administracja⁵ (ang. *e-government*) jako „Elektroniczną administrację publiczną polegającą na wykorzystaniu ICT w połączeniu ze zmianami organizacyjnymi i nowymi umiejętnościami w administracji publicznej w celu usprawnienia usług publicznych i procesów demokratycznych oraz silniejszego wsparcia programów tworzonych przez administrację publiczną”. Obecnie w jednym miejscu rozwijana jest główna platforma elektroniczna – www.gov.pl – skupiająca i integrująca wcześniejsze platformy przeznaczone dla obywatela, przedsiębiorcy, urzędnika i rolnika.

Współczesny rolnik jest w wyjątkowej sytuacji, ponieważ na platformie [gov.pl](http://www.gov.pl) może jednocześnie korzystać z e-urzędu nie tylko z pozycji obywatela i rolnika, lecz także często jako osoba prowadząca działalność gospodarczą z pozycji przedsiębiorcy.

4. System informatyczny Kasy Rolniczego Ubezpieczenia Społecznego, <https://www.ekrus.gov.pl/p4b-web/index.html>, dostęp 20.04.2022.

5. Główny Urząd Statystyczny, <https://stat.gov.pl/metainformacje/slownik-pojec/pojecia-stosowane-w-statystyce-publicznej/1769,pojecie.html>, dostęp 20.04.2022.

Przykładowe kategorie spraw możliwych do załatwienia w e-urzędzie dla obywatela⁶:

- Dokumenty i dane osobowe – dowód osobisty, paszport, prawo jazdy, dostęp i zmiana danych osobowych, dane kontaktowe;
- Edukacja – zdalne lekcje, żłobek, przedszkole, szkoła podstawowa, liceum, technikum, szkoła branżowa, studia;
- Kierowcy i pojazdy – prawo jazdy, rejestracja pojazdu, wyrejestrowanie pojazdu, kary i mandaty, parkowanie;
- Meldunek i wybory – zameldowanie stałe, zameldowanie czasowe, wymeldowanie, wybory, głosowania;
- Nieruchomości i środowisko – księgi wieczyste, dom i mieszkanie, podatki i środowisko, geodezja i kartografia;
- Podatki – podatek od: dochodu, spadku, darowizny i czynności cywilnoprawnych;
- Pomoc prawna – pomoc dla konsumentów, telefon zaufania, zgłoś przestępstwo lub wykroczenie;
- Praca i biznes – zatrudnienie, własny biznes, dofinansowania, podatki;
- Rodzina i małżeństwo – dziecko, świadczenia dla dzieci, małżeństwo, rodzina, problemy rodzinne;
- Wojsko i bezpieczeństwo – służba wojskowa, weteran, bezpieczeństwo, telefony zaufania;
- Wyjazdy i wypoczynek – ubezpieczenie, wyjazd w kraju, wyjazd za granicę, wyjazd dzieci;
- Zasiłki i pomoc finansowa – pomoc na dziecko, pomoc na mieszkanie, trudna sytuacja, zasiłki zdrowotne;
- Zaświadczenia i odpisy – akta stanu cywilnego, KRS i KRK, księgi wieczyste, rejestr dowodów osobistych;
- Zdrowie i ubezpieczenia społeczne – leczenie, rehabilitacja, niepełnosprawność, renta, emerytura, ubezpieczenia, pogrzeb;
- Cudzoziemiec w Polsce – uzyskaj numer PESEL.

Kategorie spraw możliwych do załatwienia w e-urzędzie dla przedsiębiorcy⁷:

- Tarcza Antykryzysowa – pakiet wsparcia dla przedsiębiorców w ramach programu rządowego – Tarcza Antykryzysowa;
- Zakładanie firmy – wybierz rodzaj firmy, jaką chcesz prowadzić i dowiedz się, jak ją założyć;

6. Serwis Rzeczypospolitej Polskiej, <https://www.gov.pl/web/gov/uslugi-dla-obywatela>, dostęp 20.04.2022.

7. Serwis Rzeczypospolitej Polskiej, <https://www.gov.pl/web/gov/uslugi-dla-przedsiębiorcy>, dostęp 20.04.2022.

- Rozwój firmy – sprawdź, jak rozwijać swoją firmę i gdzie znaleźć finansowanie;
- Pracownicy w firmie – sprawdź, jakie są zasady zatrudniania pracowników, ich prawa i obowiązki;
- Podatki i księgowość – dowiedz się, jak rozliczać podatki i prowadzić księgowość;
- Ubezpieczenia społeczne – zobacz, jak załatwić sprawy związane z ubezpieczeniami w ZUS/KRUS;
- Sprawy urzędowe – dowiedz się, jak załatwiać sprawy przedsiębiorcy w urzędach;
- Obowiązki przedsiębiorcy – poznaj swoje obowiązki przy prowadzeniu firmy;
- Zezwolenia, koncesje, rejestry – zezwolenia, koncesje, wpisy do rejestrów działalności regulowanej, świadectwa;
- Uprawnienia zawodowe – sprawdź, jak załatwiać sprawy związane z uprawnieniami w Twoim zawodzie;
- Zmiany w firmie – zobacz, jak przeprowadzać zmiany w firmie i jak zgłaszać je do urzędów;
- Zawieszenie i wznowienie – załatwiasz sprawy związane z zawieszaniem i wznowianiem działalności;
- Zamykanie firmy – jak załatwić sprawy związane z zamykaniem firmy, sprzedażą, dziedziczeniem, upadłością;
- Sprzedaż i marketing – poznaj zasady wprowadzania produktów/usług na rynek;
- Kontrahenci i klienci – dowiedz się, jakie są zasady rzetelnej współpracy z kontrahentami i klientami;
- Handel zagraniczny – dowiedz się, jak prowadzić handel zagraniczny w UE i poza UE;
- Prowadzenie biznesu w UE – zobacz, jak prowadzić własny biznes w krajach Unii Europejskiej;
- Inwestycje budowlane – załatwiasz formalności związane z realizacją inwestycji budowlanych w firmie;
- Cudzoziemcy w Polsce – poznaj zasady prowadzenia biznesu w Polsce przez cudzoziemców.

Kategorie spraw możliwych do załatwienia w e-urzędzie dla rolnika⁸:

- Wsparcie finansowe, dofinansowania do działalności – płatność bezpośrednia, oszacowanie strat w uprawach rolnych, podatek akcyzowy za paliwo rolnicze;
- Ubezpieczenia społeczne – emerytura, renta, zasiłek macierzyński, zasiłek pogrzebowy, ubezpieczenie zdrowotne i społeczne;
- Zaświadczenia, zezwolenia i rejestry – urzędowy rejestr podmiotów profesjonalnych, pozwolenia, materiał siewny, działalność nadzorowana;
- Uprawa roślin – świadectwo fitosanitarne, ekologiczny i konwencjonalny materiał siewny, straty w uprawach rolnych, rolnictwo ekologiczne, sprzedaż ziemi rolnej;
- Hodowla zwierząt – higiena i warunki utrzymywania zwierząt, działalność nadzorowana, ustawa zakaźna, identyfikacja i rejestracja zwierząt;
- Nieruchomości i ziemia rolna – obrót ziemią rolną, sprzedaż, kupno, portal ogłoszeniowy.

E-obywatel, oprócz powyższych kategorii spraw, ma dostęp do oddzielnych platform takich jak:

- Platforma Usług Elektronicznych ZUS (ZUS-PUE),
- Elektroniczna skrzynka podawcza (ePUAP),
- Internetowe Konto Pacjenta,
- Centralna Ewidencja i Informacje o Działalności Gospodarczej (CEIDG),
- Centralna Ewidencja Pojazdów i Kierowców (CEPIK),
- System Elektronicznych Ksiąg Wieczystych,
- Portal podatkowy,
- Geoportal itp.

Do e-swiata, do e-administracji potrzebny jest klucz, dzięki któremu obywatel może bezpiecznie potwierdzić swoją tożsamość. Kluczem otwierającym cyfrowy świat jest Profil Zaufany i/lub Podpis Kwalifikowany, które pełnią funkcję swoistych wirtualnych podpisów.

Profil Zaufany⁹ (PZ) jest bezpłatnym narzędziem udostępnionym przez państwo, dzięki któremu można wykonać następujące czynności:

- potwierdzić swoją tożsamość w systemach elektronicznej administracji,
- podpisać dokument podpisem kwalifikowanym.

8. Serwis Rzeczypospolitej Polskiej, <https://www.gov.pl/web/gov/uslugi-dla-rolnika>, dostęp 20.04.2022.

9. Serwis informacyjno-usługowy dla przedsiębiorcy, <https://www.biznes.gov.pl/pl/portal/0074>, dostęp 20.04.2022.

Profil Zaufany służy wyłącznie do kontaktów z administracją publiczną (np. urzędami, ministerstwami). Jest on ważny przez trzy lata z możliwością przedłużenia na kolejne trzy. Jest unikalny, przypisany tylko do jednego użytkownika, dlatego też nie należy go nikomu udostępniać.

Rycina 1. Informacje o Profilu Zaufanym

Masz firmę? Podpisz JPK_VAT profilem zaufanym

Pobierz bezpłatną aplikację | Podpisz Profilem Zaufanym

01 Co to jest Profil Zaufany?

Profil Zaufany to **bezpłatne narzędzie**, dzięki któremu można załatwiać sprawy urzędowe **online** w serwisach administracji publicznej, **bez wychodzenia z domu**.

Teraz możesz założyć i potwierdzić Profil Zaufany online za pośrednictwem **bankowości elektronicznej**

Dodatkowo, możesz założyć Profil Zaufany przez internet i potwierdzić go w **Punkcie Potwierdzającym**

02 Jak założyć i potwierdzić?

24h/7 dni w tygodniu – Profil Zaufany możesz założyć i potwierdzić w pełni online przy pomocy **zewnętrznego dostawcy tożsamości**, np. banku

krok 1 W systemie bankowości elektronicznej twojego banku, **wypełnij formularz o założenie Profilu Zaufanego**

krok 2 Operację potwierdź **bankowym kodem autoryzacyjnym**. Na Twój adres mailowy otrzymasz potwierdzenie założenia konta

03 Co mogę załatwić?

- Zalogować do **Internetowego Konta Pacjenta** (IKP)
- Podpisać **JPK_VAT**
- Złożyć wniosek o **rejestrację działalności gospodarczej**
- Wystąpić o **Europejską Kartę Ubezpieczenia Zdrowotnego**
- Załatwić **sprawy urzędowe** dla swojej rodziny: beczkowe, świadczenia rodzicielskie, Karta Dużej Rodziny, Świadczenie o Funduszu Alimentacyjnym
- Uzyskać **odpis aktu stanu cywilnego**
- **Dziesiątki innych spraw**

Źródło: Profil Zaufany, <https://pz.gov.pl/pz/index>, dostęp 20.04.2022.

Od powstania PZ (2011 roku) minęło już ponad dziesięć lat, do 2016 roku korzystali z niego przede wszystkim urzędnicy (ok. 400 tys. kont PZ). W 2019 roku założyli ich tylko trzy miliony. Od 2020 roku nastąpiła diametralna zmiana, od tego czasu notuje się ogromny wzrost zakładanych PZ. Na koniec 2020 roku było już osiem milionów aktywnych kont PZ. W marcu 2022 roku ich liczba sięgnęła barierę 14 milionów, a tylko od początku bieżącego roku obywatele założyli 600 tys. nowych PZ¹⁰.

Podpis Kwalifikowany¹¹ (PK) ma szersze zastosowanie niż PZ. Nie ogranicza się tylko do spraw urzędowych, dzięki niemu można zawierać umowy na odległość i brać udział w przetargach. Ma moc prawną taką samą jak podpis własnoręczny i jest usługą płatną, dlatego też jest najczęściej używany przez prywatne firmy.

10. Dane Kancelarii Prezesa Rady Ministrów z dnia 10 marca 2022 r., Serwis Rzeczypospolitej Polskiej, <https://www.gov.pl/web/cyfryzacja/14-milionow-profilu-zaufanych2>, dostęp 5.05.2022.

11. Serwis informacyjno-usługowy dla przedsiębiorcy, <https://www.biznes.gov.pl/pl/portal/0075>, dostęp 20.04.2022.

Polska nie poprzestała na powyższych narzędziach identyfikujących i uwierzytelniających. W dniu 4 marca 2019 roku zostało wprowadzone rozwiązanie polegające na wbudowaniu warstwy elektronicznej (chipu) do wszystkich nowo wydawanych dowodów osobistych (e-dowody). Do użycia e-dowodu potrzebny jest specjalny czytnik podłączony do komputera lub telefon wyposażony w technologię NFC (ang. *Near Field Communication*, czyli komunikacja bliskiego zasięgu). Posiadając odpowiedni czytnik obsługujący e-dowód, sprawnie i wygodnie logujemy się do e-usług portali administracji publicznej bez loginu i bez hasła. Wbudowana w dowód osobisty warstwa elektroniczna umożliwia podpisywanie dokumentów wysyłanych elektronicznie (dzięki podpisowi osobistemu).

Rozbudowywanie dalszej infrastruktury informacyjno-komunikacyjnej pozwoliło na stworzenie specjalnej aplikacji na telefony – mObywatel¹². Aplikacja ta poszła o krok dalej w cyfryzacji naszego życia, od tej pory mamy ciągły dostęp do e-administracji poprzez telefon.

mObywatel jest rodzajem cyfrowego portfela zawierającego dokumenty i umożliwiającego dostęp do e-usług. Aplikacji ta umożliwia:

- bezpiecznie pobieranie i okazywanie swoich danych,
- szybkie i skuteczne zalogowanie się do e-Urzędu Skarbowego i rozliczenie PIT-u,
- bezpieczną realizację eRecepty bez podawania numeru PESEL,
- realizację zniżek, korzystanie z przywilejów dla dużych rodzin,
- okazanie potwierdzenia szczepienia przeciwko COVID-19,
- okazanie prawa jazdy kierowców i sprawdzenie swoich punktów karnych,
- okazanie i sprawdzenie danych swojego samochodu,
- korzystanie z mLegitymacji szkolnej lub studenckiej.

Tabela 1. Osoby korzystające z aplikacji mObywatel w 2021 roku

Wyszczególnienie	Osoby korzystające z aplikacji mObywatel
Ogółem	5 484 806
w tym	
Unijny certyfikat Covid	4 429 933
mPrawo jazdy	3 294 120
mPojazd	2 300 466

Źródło: Główny Urząd Statystyczny, <https://stat.gov.pl/obszary-tematyczne/nauka-i-technika-spolnoczenstwo-informacyjne/spolnoczenstwo-informacyjne/spolnoczenstwo-informacyjne-w-polsce-w-2021-roku,1,15.html>, dostęp 2.05.2022.

12. Serwis Rzeczypospolitej Polskiej, <https://www.gov.pl/web/mobywatel>, dostęp 20.04.2022.

W całym 2021 roku odsetek osób w wieku pomiędzy 16 lat i 74 lata korzystających z usług e-administracji publicznej wyniósł 47,5% – i jest to wzrost o 5,6 punktów procentowych w porównaniu do roku poprzedniego¹³. W grupie czynności wykonywanych on-line największy wzrost zanotowano w wysyłaniu wypełnionych formularzy – wzrost o 6,4 punktów procentowych w porównaniu do roku poprzedniego. O około 2 punkty procentowe wzrosło np. przeglądanie informacji na stronach administracji publicznej. Z roku na rok powiększa się także grupa osób aktywnie kontaktujących się z różnymi urzędami w celu załatwienia swoich spraw.

Tabela 2. Osoby korzystające z usług administracji publicznej za pomocą Internetu

Wyszczególnienie	2020 rok	2021 rok
Osoby korzystające z usług administracji publicznej za pomocą Internetu	41,9%	47,5%
w celu:		
wyszukiwania informacji na stronach administracji publicznej	27,2%	29,4%
pobierania formularzy urzędowych	25,4%	27,4%
wysyłania wypełnionych formularzy	33,5%	39,9%

Źródło: Główny Urząd Statystyczny, Broszura informacyjna pt. „Społeczeństwo informacyjne w Polsce w 2021 roku. Informacja sygnałna”, www.stat.gov.pl, dostęp 27.04.2022.

Liczba osób korzystających z e-administracji systematycznie wzrasta z roku na rok. Włączenie szerzej społeczeństwa w proces cyfryzacji państwa ma istotne znaczenie społeczne i ekonomiczne, zapobiega wykluczeniu cyfrowemu, zwiększa dostępność e-usług instytucji państwowych oraz zmniejsza kolejki w urzędach. Wiąże się z tym również wykształcenie odpowiednich e-kompetencji i stworzenie bezpiecznego środowiska użytkownika. E-administracja to przede wszystkim szybki dostęp do informacji, wygoda interesantów, oszczędność czasu oraz jednakowa, wysoka jakość obsługi. Za cyfryzacją przemawiają zarówno aspekty ekonomiczne, jak i postrzeganie Polski w lepszym świetle przez inwestorów zagranicznych. Według raportu McKinsey & Company z 2018 roku pt. „Polska jako Cyfrowy Challenger – Cyfryzacja nowym motorem wzrostu dla kraju i regionu”¹⁴ dzięki cyfryzacji do 2025 roku PKB Polski może wzrosnąć o dodatkowe 64 mld euro i osiągnąć 15% PKB.

13. Główny Urząd Statystyczny, <https://stat.gov.pl/obszary-tematyczne/nauka-i-technika/spoleczenstwo-informacyjne/spoleczenstwo-informacyjne-w-polsce-w-2021-roku,2,11.html>, dostęp 27.04.2022.

14. McKinsey & Company, <https://www.mckinsey.com/pl/our-insights/polska-jako-cyfrowy-challenger>, dostęp 5.05.2022.

eKRUS – Portal dla Rolników

Pod nazwą eKRUS¹⁵ kryje się system informatyczny Kasy Rolniczego Ubezpieczenia Społecznego powszechnie dostępny przez Internet, a jego celem jest obsługa on-line ubezpieczonych w Kasie.

eKRUS został stworzony dla:

- rolników i małżonków rolników;
- domowników, podlegających ubezpieczeniu społecznemu rolników (USR) lub ubezpieczeniu zdrowotnemu (UZ);
- członków rodzin zgłoszonych do ubezpieczenia zdrowotnego.

Początkowo od 3 lipca 2015 roku Portal dla Rolników eKRUS został pilotażowo wdrożony w Oddziale Regionalnym KRUS w Rzeszowie i jego podległych placówkach terenowych, następnie od 2016 roku w całej Kasie.

Aby móc korzystać z Portalu dla Rolników, należy zarejestrować się i utworzyć profil użytkownika. Można tego dokonać trzema drogami:

- w formie wniosku drukowanego – trzeba go wypełnić i wydrukować ze strony, opatrzyć własnoręcznym podpisem i złożyć w Placówce Terenowej KRUS lub wypełnić bezpośrednio w Placówce;
- w formie wniosku elektronicznego – jest to najłatwiejsza metoda polegająca na podaniu własnego adresu poczty elektronicznej i podpisaniu formularza swoim Profilem Zaufanym;
- w formie wniosku ePUAP – należy zalogować się do platformy ePUAP, następnie wskazać odpowiedni urząd, wyszukać wniosek i go wypełnić. Wniosek potwierdza się Profilem Zaufanym lub innym podpisem elektronicznym i przekazuje się go dalej trybem elektronicznym do rozpatrzenia przez Usługodawcę.

Logując się po raz pierwszy do systemu eKRUS, należy wprowadzić nazwę użytkownika (login) oraz hasło i je zaakceptować. Użytkownik będzie musiał zmienić hasło na inne również bezpieczne i uzupełnić pytanie pomocnicze wraz z odpowiedzią na nie. Odpowiedź na to pytanie będzie potrzebna w sytuacji odzyskiwania dostępu do konta. W przypadku przekroczenia limitu prób logowania, tzn. podawania błędnego loginu lub/i hasła, system zablokuje konto użytkownika. Dostęp do konta można odzyskać przy pomocy funkcji odzyskiwania konta lub skorzystać z logowania przez login.gov.pl. Dodatkowo konto można odzyskać poprzez kontakt z pomocą techniczną lub lokalną Placówką Terenową KRUS.

15. System informatyczny Kasy Rolniczego Ubezpieczenia Społecznego, <https://www.ekrus.gov.pl/p4b-web/index.html>, dostęp 10.05.2022.

Wszystkie potrzebne informacje począwszy od metod założenia profilu użytkownika platformy eKRUS aż do sposobów bieżącej obsługi zawarte są w przewodniku umieszczonym w sekcji Niezbędnik pod linkiem Przewodnik po eKRUS (w formie dokumentu PDF)¹⁶.

Portal dla Rolników eKRUS jest cały czas rozwijany, rozbudowywany i wzbogacany o nowe możliwości i funkcje. Po zalogowaniu się do profilu użytkownika mamy dostęp do informacji, dokumentów i funkcji dotyczących m.in.:

- daty ostatniej wizyty na portalu i nieudanych logowań;
- terminu płatności składek i ich wysokości;
- zestawienia sald składek;
- zestawienia zadłużeń;
- informacji o możliwym ustaniu ubezpieczenia społecznego – ubezpieczenia na wniosek;
- danych osobowych;
- wygenerowania dokumentów takich jak: (1) zaświadczenia o podleganiu USR, (2) zaświadczenia o okresach podlegania USR, (3) zaświadczenia o okresach podlegania i opłaceniu składek UZ;
- przeglądania okresów ubezpieczenia i wykazu składek ubezpieczeniowych (zapłaconych/niezapłaconych);
- przeglądania listy spraw z zakresu USR;
- przeglądania przypomnień i upomnień;
- spraw dot. pomocnika rolnika;
- przeglądania skrzynki wiadomości kierowanych do ubezpieczonego;
- płatności składek oraz zadłużeń z tytułu USR i UZ.

Portal dla Rolników eKRUS jest jedną z nielicznych platform e-usług publicznych, która na swojej stronie umieściła solidnie opisane Zasady Bezpieczeństwa¹⁷, którymi powinien kierować się każdy użytkownik. Należy wyróżnić powyższą platformę, ponieważ w swoich zasadach dotyczących bezpieczeństwa zwróciła uwagę na to, jak ważne jest sprawdzenie poprawności adresu URL strony (ang. *Uniform Resource Locator* – ujednolicony format adresowania) przed logowaniem i jej certyfikatu SSL (ang. *Secure Sockets Layer* – warstwa bezpiecznych gniazd), który służy do poświadczenia autentyczności serwera. Zasady bezpieczeństwa w sieci zostaną dokładniej omówione w następnym podrozdziale.

16. System informatyczny Kasy Rolniczego Ubezpieczenia Społecznego, https://www.ekrus.gov.pl/p4b-web/static/eKRUS_Przewodnik_20220428.pdf, dostęp 10.05.2022.

17. System informatyczny Kasy Rolniczego Ubezpieczenia Społecznego, <https://www.ekrus.gov.pl/p4b-web/zasadyBezpieczenstwa.html>, dostęp 10.05.2022.

Na koniec pierwszego kwartału 2022 roku było 14 mln. aktywnych użytkowników PZ na 38 028 000¹⁸ obywateli Polski, co stanowi prawie 37% populacji naszego kraju. Mając na uwadze 3,82% użytkowników platformy eKRUS względem ogółu ubezpieczonych w KRUS, mamy świadomość, jak wiele jest jeszcze do zrobienia w tej materii. Jak wielki potencjał drzemie w tej grupie społecznej, którą są rolnicy.

Tabela 3. Osoby korzystające z platformy eKRUS

Rok	Liczba ubezpieczonych ogółem	Liczba profili użytkownika na platformie eKRUS	Procent użytkowników eKRUS względem ogółu ubezpieczonych
2019	1 199 285	25 445	2,12%
2020	1 173 236	32 596	2,78%
2021	1 134 603	39 500	3,48%
31.03.2022	1 127 508	43 084*	3,82%

*Dane na dzień 24 maja 2022 roku.

Źródło: Opracowanie własne na podstawie: Broszura statystyczna pt. „KRUS w liczbach 2019–2021”, <https://www.krus.gov.pl/wydawnictwa/broszury-informacyjne-o-krus/>, dostęp 15.05.2022; Kasa Rolniczego Ubezpieczenia Społecznego, Podstawowe dane statystyczne z zakresu ubezpieczonych, <https://www.krus.gov.pl/krus/krus-w-liczbach/podstawowe-dane-statystyczne-z-zakresu-ubezpieczonych/>, dostęp 15.05.2022; Informacje pozyskane z Biura Informatyki i Telekomunikacji Centrali KRUS, dostęp 24.05.2022.

Bezpieczeństwo w sieci

Bezpieczeństwo ogólnie pojętej sieci internetowej zależy od człowieka. Często słyszymy, że człowiek jest najsłabszym ogniwem tej skomplikowanej struktury, którą jest cyberbezpieczeństwo. Z powyższym stwierdzeniem należy zgodzić się tylko połowicznie, ponieważ człowiek może i jest najsłabszym ogniwem tej układanki, ale jednocześnie może stać się jej najmocniejszym elementem. Aby tak się stało, należy zdobywać i cały czas rozwijać kompetencje cyfrowe, znać podstawy bezpieczeństwa w sieci i być na bieżąco z nowymi zagrożeniami. Nie jest to trudne przy dzisiejszym swobodnym dostępie do informacji. Zazwyczaj problem ze zrozumieniem zasad cyberbezpieczeństwa wiąże się z brakiem podstaw w tym zakresie. Wychodząc naprzeciw temu problemowi, poniżej przedstawiono podstawowe informacje z zakresu e-bezpieczeństwa.

Złośliwe oprogramowanie (ang. *malware*) możemy podzielić na różne typy, kategorie, mechanizmy działania czy sposoby infekcji.

18. Główny Urząd Statystyczny, <https://stat.gov.pl/podstawowe-dane/>, dostęp 27.05.2022.

Rodzaje malware¹⁹

1. Robaki (ang. *worms*) – to programy, które szybko się rozmnażają i rozprzestrzeniają w sieci, wykorzystując one błędy, luki i podatności (tak zwane eksploity) w systemach operacyjnych, zwłaszcza w tych, które nie były aktualizowane.
2. Trojany (tzw. konie trojańskie, ang. *Trojan Horse*) – to oprogramowania, które podszywając się pod przydatne lub ciekawe programy, aplikacje oszukują użytkownika. Po uruchomieniu ten początkowo niegroźny plik ujawnia swój złośliwy charakter, wykradając dane, ściągając inne złośliwe programy czy dając przestępcy zdalny dostęp do komputera. Przykładem jest trojan bankowy – umożliwiający wykradanie pieniędzy użytkowników z bankowości elektronicznej.
3. Wirusy (ang. *virus*) – dopisują swój złośliwy kod do innych plików wykonywalnych systemu operacyjnego, posiadają zdolność powielania się i rozprzestrzeniania na inne systemy.
4. Błędy (ang. *bugs*) – błędy, usterki oprogramowania, które mogą zakłócać działanie programów, mogą stanowić luki w zabezpieczeniach i być wykorzystane do uszkodzenia lub przejęcia systemu operacyjnego.
5. Ransomware (ang. *ransom*, okup) – to oprogramowanie szyfrujące wszystkie pliki na dyskach w celu żądania okupu, zaszyfrowanie uniemożliwia dostęp do systemów komputerowych.
6. Spyware (ang. *spy*, szpieg, szpiegować) – to oprogramowanie szpiegujące, monitorujące aktywność na komputerze, np. keylogger, który rejestruje pisanie na klawiaturze.
7. Spambots – zautomatyzowane programy zaprojektowane do wysyłania niechcianych e-maili (spamu).
8. Adware – to oprogramowanie reklamowe, które wyświetla niechciane treści reklam. Takie reklamy mogą być wykorzystane przez przestępców, wabiąc treścią, kliknięcie w nie może przekierowywać na niebezpieczne strony lub instalować niebezpieczne programy.
9. Auto-dialery – to program służący do automatycznego wykonywania połączeń telefonicznych.

Współcześnie duża część przestępstw związanych z nowymi technologiami bazuje na sztuczkach socjotechnicznych, polegających na wywieraniu wpływu na ludzi, stosowaniu perswazji w celu dokonania oszustwa. Aktualna wiedza o nowych sposobach przestępstw jest jak niewidzialna tarcza chroniąca społeczeństwo przed takimi zagrożeniami.

19. Portal KapitanHack.pl, <https://kapitanhack.pl/2019/01/08/malware/rodzaje-malware-i-sposoby-na-ich-wykrycie-oraz-ochrone/>, dostęp 29.05.2022.

Najczęstsze metody cyberataków^{20, 21}

1. **Phishing** (łowienie) – jedna z najpopularniejszych metod ataku, polega m.in. na wyłudzeniu danych do logowania, np. do banku, skrzynki e-mailowej, mediów społecznościowych, wszelkiego rodzaju serwisów, jak również do ściągnięcia złośliwego oprogramowania. Następuje ono najczęściej poprzez e-mail, SMS, stronę i/lub komunikator internetowy i ma na celu skłonić do kliknięcia w link, ściągnięcia i otworzenia załącznika, zalogowania się na stronie imitującej prawdziwy serwis czy podania danych osobowych, danych karty kredytowej itp.
2. **Spear-phishing** – jest to atak ukierunkowany na konkretną osobę.
3. **Smishing** – rodzaj phishingu, wiadomość wysłana z bramki internetowej podszywająca się pod usługodawców, np. bank, dostawcę prądu. W serwisie internetowym, przez który wysyła się SMS-y, można podać każdy dowolny numer telefonu. Powoduje to odbieranie takich wiadomości w tym samym miejscu co SMS-y, np. z banku. Wiadomość ta najczęściej nakłania do kliknięcia w link.
4. **Spoofing**²² – polega na podszywaniu się pod inny numer telefonu, np. z banku, urzędu i wykonaniu połączenia do atakowanej osoby. Nieświadoma osoba widzi na telefonie numer, np. z banku, dochodzi wtedy najczęściej do wyłudzenia danych osobowych, danych bliku, numeru karty kredytowej, danych logowania do kont on-line czy niekorzystnego rozporządzenia własnym mieniem. W tym celu używa się komunikatorów internetowych.
5. **Vishing**²³ – jest phishingiem głosowym, nie wymaga od przestępców wiedzy informatycznej. Celem jest zdobycie poufnych informacji lub/i nakłonienie ofiary do wykonania określonego zadania, np. zainstalowania aplikacji na telefonie, komputerze czy przekazanie kosztowności osobie udającej policjanta.
6. **Whaling** – oszust podaje się za kogoś ważnego, np. dyrektora, podszywa się pod osoby na wyższych stanowiskach. Najczęściej nakłania ofiarę do wykonania zadania, np. wykonania przelewu pieniędzy, ujawnienia danych osobowych czy firmowych.
7. **Pharming**²⁴ – jest zaawansowanym informatycznie rodzajem phishingu bez elementu socjotechnicznego. Jest on bardzo niebezpieczny ze względu na metodę

20. Zespół CERT Polska, <https://cert.pl/posts/2022/05/krajobraz-bezpieczenstwa-polskiego-internetu-w-2021-roku/>, dostęp 9.05.2022.

21. Zespół CERT Polska, https://cert.pl/uploads/docs/Raport_CP_2020.pdf, dostęp 9.05.2022.

22. Niebezpiecznik.pl, <https://niebezpiecznik.pl/post/cyberalerty-darmowa-aplikacja-od-niebezpiecznika-ostrzegajaca-o-atakach/>, dostęp 30.05.2022.

23. Krajowy Instytut Cyberbezpieczeństwa, <https://kicb.pl/spoofing-i-vishing-poznaj-ich-tajniki-i-nie-daj-sie-oszustom/>, dostęp 29.05.2022.

24. Avast Software, <https://www.avast.com/pl-pl/c-pharming>, dostęp 29.05.2022.

przebiegu ataku. Jedyną ochroną przed nim jest dobre oprogramowanie antywirusowe. Metoda ta polega na przekierowywaniu na fałszywe strony internetowe podszywające się pod inne legalne i zaufane witryny. Na telefonach tworzona jest nakładka na aplikacje bankowe. W ten sposób wykradane są dane do logowania, np. do bankowości internetowej.

Powyższa lista nie wyczerpuje wszystkich metod dokonywania oszustw, ale wskazuje na główne ich kierunki i metody. Ofiara jest zawsze nakłaniana do działania czy to ze strachu i ciekawości, czy chciwości. Oszust specjalnie wywiera presję, by zmniejszyć czas do namysłu i nakłonić ofiarę do wykonania określonych czynności.

Zagrożenia

Na świecie i w Polsce systematycznie są przeprowadzane kampanie phishingowe i wszelkiego rodzaju oszustwa z wykorzystaniem sztuczek socjotechnicznych i/lub związanych z zainstalowaniem niechcianego, złośliwego oprogramowania, które wykrada poufne dane, daje zdalny dostęp do urządzenia²⁵.

Przykładowe kampanie:

1. SMS-y, e-maile od przestępców imitujące banki, dostawców usług (np. PGE, Energa, DHL, inPost) czy sklepy internetowe nakłaniające do kliknięcia w fałszywy link, ściągnięcie i instalację złośliwego oprogramowania. W ten sposób przestępcy przejmują telefon, komputer i wykradają umieszczone na urządzeniach dane umożliwiające logowanie się do różnych serwisów, banków, poczty internetowej. Linki przekierowują również do fałszywych bramek płatności, wykradając dane karty kredytowej, debetowej.
2. SMS-y od mObywatela (imitujące prawdziwą aplikację) informujące o kolejnej dawce szczepienia lub wygranej w loterii narodowej nakłaniające do zainstalowania złośliwego oprogramowania, podobnie wyglądało oszustwo SMS-owe z informacją o COVID-19.
3. Reklamy na portalach społecznościowych informujące o możliwości uzyskania pieniędzy po podjęciu akcji na wskazanej stronie, np. wpisz nr klienta i uzyskaj dodatkowe środki na konto czy poleć konto bankowe znajomemu i odbierz środki. Atak ten wymusza podanie danych do konta lub karty kredytowej, jej daty ważności i kodu CVC.
4. Reklamy na portalach społecznościowych zachęcające do inwestycji np. w Orlen, kryptowaluty. Ta forma oszustwa wymusza zakładanie fikcyjnych kont, podanie danych osobowych i finansowych lub instalację złośliwego oprogramowania.

25. Zespół CERT Polska, <https://cert.pl/zagrozenia/>, dostęp 29.05.2022.

5. Reklamy w rezultatach wyszukiwarek, cyberprzestępcy wykorzystują mechanizmy reklamowania i próbują podmienić wynik wyszukiwania, aby skierować ofiarę ataku na fałszywą stronę.
6. E-maile z załącznikami, które należy ściągnąć, np. faktury, regulaminy sklepów internetowych, aktualizacje regulaminów czy polityki RODO itp. W tym przypadku istnieje ryzyko ściągnięcia złośliwego oprogramowania, włączenia makra w plikach Excel zezwalającego na instalację malware.
7. Oszustwa na portalach ogłoszeniowych zazwyczaj związane są z komunikowaniem się ze sprzedawcą poza oficjalnym kanałem kontaktowym i nakłanianiem ofiary ataku do odebrania środków za towar, w tej sytuacji atakowany przekierowany jest na fałszywą stronę bankową i podaje swoje dane do konta bankowego.
8. Zachęcanie treścią do odwiedzenia fałszywych stron, najczęściej ukazujących się na serwisach społecznościowych, np. gwałt na nieletniej, policja prosi o pomoc, atak rakietowy na Polskę, piłkarz zarobił krocie. Wszystkie te informacje mają za zadanie wzbudzić ciekawość, zbulwersować. Klikając w nie, jesteśmy przekierowywani na strony z fałszywym panelem logowania. W ten sposób możemy stracić konto społecznościowe, które następnie zostanie wykorzystane do wyłudzenia pieniędzy od naszych znajomych. W podobny sposób działa oszustwo „pomoc przy głosowaniu” na portalach społecznościowych.

Dobre praktyki

Poniższe zasady opracowano na podstawie materiałów umieszczonych na stronie Zespołu CERT Polska (<https://cert.pl/>) i zasad bezpieczeństwa umieszczonych na platformie eKRUS (<https://www.ekrus.gov.pl>). Dotyczą one komputerów, telefonów, routerów, jak również innych urządzeń elektronicznych.

1. Aktualizuj oprogramowanie systemów operacyjnych i przeglądarek internetowych na swoich urządzeniach, stwórz indywidualne konta użytkowników mające mniejsze uprawnienia niż administrator, włącz firewall.
2. Używaj oprogramowania antywirusowego z rozszerzonym pakietem narzędzi, np. typu Internet Security, chronią one dodatkowo przed innymi zagrożeniami.
3. Aktualizuj oprogramowanie (ang. *firmware*) routera, włącz firewall i zmień domyślne hasło administratora, utwórz hasło dostępu do sieci WiFi; zaleca się również włączenie sieci dla gości.
4. Instaluj oprogramowanie tylko od legalnych i pewnych wydawców, unikaj instalowania oprogramowania niewiadomego pochodzenia.
5. Zabezpiecz swoje hasła i loginy do różnych aplikacji przed nieuprawnionym dostępem, pod żadnym pozorem nikomu ich nie udostępniaj.

6. Stosuj długie hasła zawierające co najmniej 14 różnych znaków (cyfry, duże i małe litery, znaki specjalne), unikaj hasel z twoimi danymi, mogą być one publicznie znane.
7. Nie używaj tego samego hasła więcej niż raz i do wielu usług, w razie wycieku wszystkie konta z tym hasłem mogą być przejęte, cyklicznie zmieniaj hasła.
8. Gdy używasz wielu loginów i hasel, zaleca się skorzystanie z menadżera hasel.
9. Gdzie tylko to możliwe, włącz uwierzytelnianie dwuskładnikowe, np. poczty elektronicznej i kont społecznościowych, zapobiega to przejęciu kont. Tylko token sprzętowy U2F²⁶ (np. YubiKey) jest odporny na ataki phishingowe.
10. Logując się na stronie internetowej, zawsze sprawdź poprawność adresu URL. Pamiętaj, że kłódka przed adresem świadczy wyłącznie, że połączenie pomiędzy twoim urządzeniem a serwerami aplikacji jest szyfrowane protokołem SSL (https, gdzie „s” to skrót od „secure”), dlatego zawsze dodatkowo sprawdź certyfikat SSL strony.
11. Włącz w przeglądarkach dodatkowe narzędzia bezpieczeństwa, wyłącz automatyczne zapisywanie hasel.
12. Pamiętaj o wylogowaniu się z serwisu i zamknięciu okna przeglądarki, nie zostawiaj bez opieki urządzenia, na którym jesteś zalogowany do e-usług.
13. W przypadku przesyłania drogą elektroniczną ważnych dokumentów zaszyfruj je przed wysłaniem, np. programem 7-zip, hasło do dokumentu prześlij inną drogą.
14. Ignoruj wszelkie prośby o podanie loginów, hasel, danych osobowych przesłane drogą elektroniczną i przez telefon.
15. Zawsze weryfikuj nadawcę wiadomości zmuszających cię do natychmiastowego działania innym kanałem teleinformatycznym.
16. Podejrzane wiadomości w skrzynce pocztowej można przesłać do CERT Polska (<https://incydent.cert.pl>), wiadomości SMS zawierające nieznane linki można przesłać pod numer 799 448 084.
17. Opcjonalnie zainstaluj bezpłatną aplikację CyberAlerty od Niebezpiecznika dostępną w sklepie Google Play i Apple AppStore i otrzymuj ostrzeżenia o nowych zagrożeniach²⁷.

26. Serwis Sekurak, <https://sekurak.pl/poradnik-o-kluczach-sprzetowych-na-przykladzie-yubikey-5-nfc-2fa-u2f-fido2/>, dostęp 30.05.2022.

27. Niebezpiecznik.pl, <https://niebezpiecznik.pl/post/cyberalerty-darmowa-aplikacja-od-niebezpiecznika-ostregajaca-o-atakach/>, dostęp 23.08.2022.

Podsumowanie

Głównym celem opracowania było przedstawienie szans i zagrożeń w rozwoju e-usług w grupie społecznej, jaką są rolnicy. W ostatnich latach nastąpiło przyspieszenie rozwoju e-administracji w Polsce, wprowadzono nowe rozwiązania. Rozszerzono zakres spraw możliwych do załatwienia w formule on-line. Wielu obywateli szczególnie podczas okresu pandemii dostrzegło pozytywne strony w kontaktach z e-urzędem. Wygodny, bezkolejkowy system obsługi zdobywa coraz większe grono użytkowników. W 2020 roku odsetek osób korzystających z usług administracji publicznej za pomocą Internetu wynosił 41,9%, w kolejnym roku nastąpił wzrost o 5,6%, by osiągnąć poziom 47,5%. Obecnie z aplikacji mObywatel korzysta ponad 5,5 mln Polaków. Najbardziej imponujący wzrost dotyczył liczby założonych Profili Zaufanych pod koniec pierwszego kwartału bieżącego roku, tj. 14 mln aktywnych kont PZ. Nie wolno również zapomnieć, że Kasa Rolniczego Ubezpieczenia Społecznego dokłada swoją cegiełkę do rozwoju e-administracji w Polsce. Platforma eKRUS jest cały czas rozbudowywana o nowe funkcjonalności, zwiększa się liczba możliwych do pozyskania dokumentów, można również dokonać płatności. Platforma jest przejrzysta i intuicyjna. W kwietniu br. wprowadzono do niej rozwiązanie eliminujące błędy powstające podczas zakładania konta w Portalu dla Rolników eKRUS, tj. wprowadzono dodatkowe pole z powtórzonym adresem e-mail i jego potwierdzeniem. Ta mała zmiana wyeliminowała błędy w przekazywanych przez rolników adresach e-mail.

Profil Zaufany, który jest swoistym kluczem do e-usług naszego państwa posiada około 37% Polaków. Z roku na rok liczba zakładanych nowych PZ rośnie, proces ten przyspieszył szczególnie w okresie pandemii. Tak wysokiego wzrostu nie obserwujemy natomiast w liczbie zakładanych kont w Portalu dla Rolnika eKRUS. Zaledwie 3,82% użytkowników platformy eKRUS względem ogółu ubezpieczonych w KRUS wygląda jak błąd statystyczny. Pokazuje to, jak wiele jest jeszcze do zrobienia w tej sferze, śmiem stwierdzić, że może to wymagać zmian pokoleniowych. Nie czekając jednak na wymianę pokoleniową, możemy rozpocząć wśród rolników proces, który doprowadzi do osiągnięcia zakładanych celów.

„Wszystko jest trudne zanim stanie się łatwe”

Boimy się czegoś, czego nie rozumiemy, wiedza jest swoistą tarczą. Tylko rozwój kompetencji cyfrowych w grupie społecznej rolników zapewni im tę przysłowiową tarczę. Edukacja cyfrowych kompetencji powinna wykraczać poza instytucję, jaką

jest KRUS i angażować lokalne samorządy i inne instytucje państwowe. Podczas rozmów z rolnikami bardzo często można usłyszeć cyt.: to jest trudne; nie rozumiem tego; boję się; nowa dodatkowa rzecz, którą trzeba samemu ogarnąć. Ilekroć jest to wypowiedziane, nasuwa się pytanie – co można z tym zrobić? Można wiele, np. wypracować schematy zdobywania kompetencji cyfrowych na podstawie już istniejących i skierować rolników we właściwą stronę, by rozpocząć ten proces.

Należy podkreślić, że do osiągnięcia sukcesu w cyfrowej transformacji niezbędne jest zaufanie obywateli do nowych technologii, ich zrozumienie i bezpieczne użytkowanie. Niniejsza praca nie tylko przybliży e-rozwiązania e-państwa, lecz także przedstawia zagrożenia związane z elektronizacją życia codziennego oraz metody i sposoby przeciwdziałania takim niebezpieczeństwom.

W celu zwiększenia bezpieczeństwa użytkowników platformy eKRUS proponuję wprowadzenie uwierzytelniania dwuskładnikowego podczas logowania do systemu. Są różne rozwiązania – SMS-y, aplikacje uwierzytelniające, tokeny sprzętowe U2F. Dwie pierwsze metody nie chronią użytkownika przed fałszywymi stronami, które tylko przypominają tę właściwą. Dla większości nietechnicznych osób trudno jest wskazać prawdziwą domenę i odróżnić ją od fałszywej. Z pomocą przychodzą klucze kryptograficzne – tokeny sprzętowe U2F. Jeżeli rolnicy zostaliby wyposażeni w odpowiednio przygotowane tokeny sprzętowe U2F, logowanie do platformy eKRUS mogłoby odbywać się bezhasłowo, bezpiecznie i szybko. Obecnie w USA zaleca się odejście od autoryzowania dostępu do konta i transakcji bankowych za pomocą SMS-ów w kierunku bezpieczniejszych form. Bank of America jako jeden z pierwszych na świecie wprowadził tokeny sprzętowe U2F do logowania do swojego serwisu. Tak więc tylko połączenie wszystkich komponentów: edukacji, bezpieczeństwa, wygody może przynieść wymierne efekty w postaci zwiększenia liczby użytkowników platformy eKRUS. Przygotowanie rolników i wyposażenie ich w odpowiednie kompetencje cyfrowe nie tylko wpłynie pozytywnie na samą Kasę, lecz także przyspieszy cyfryzację rolnictwa i stanie się kolejnym dodatkowym motorem gospodarczym. Kasa może być pionierem w rozwijaniu bezpiecznego i łatwego dostępu do swoich usług, wprowadzając nowoczesne rozwiązanie, takie jak U2F i przeprowadzając, przy współpracy z innymi instytucjami, odpowiednie szkolenia rolników.

Za korzystaniem z zintegrowanej platformy eKRUS przemawia wygoda i szybki dostęp o każdej porze dnia do usług świadczonych na rzecz rolników przez KRUS, a także oszczędność czasu i pieniędzy.

Bibliografia

- Avast Software**, <https://www.avast.com/pl-pl/c-pharming>, dostęp 29.05.2022.
- Główny Urząd Statystyczny**, <https://stat.gov.pl/metainformacje/sloownik-pojec/pojecia-stosowane-w-statystyce-publicznej/1769,pojecie.html>, dostęp 20.04.2022.
- Główny Urząd Statystyczny**, <https://stat.gov.pl/obszary-tematyczne/nauka-i-technika-spolnoczenstwo-informacyjne/spolnoczenstwo-informacyjne/spolnoczenstwo-informacyjne-w-polsce-w-2021-roku,2,11.html>, dostęp 27.04.2022.
- Główny Urząd Statystyczny**, <https://stat.gov.pl/obszary-tematyczne/nauka-i-technika-spolnoczenstwo-informacyjne/spolnoczenstwo-informacyjne/spolnoczenstwo-informacyjne-w-polsce-w-2021-roku,1,15.html>, dostęp 2.05.2022.
- Główny Urząd Statystyczny**, <https://stat.gov.pl/podstawowe-dane/>, dostęp 27.05.2022.
- Kasa Rolniczego Ubezpieczenia Społecznego**, <https://www.krus.gov.pl/wydawnictwa/broszury-informacyjne-o-krus/>, dostęp 15.05.2022.
- Kasa Rolniczego Ubezpieczenia Społecznego**, <https://www.krus.gov.pl/krus/krus-w-liczbach/podstawowe-dane-statystyczne-z-zakresu-ubezpieczonych/>, dostęp 15.05.2022.
- Krajowy Instytut Cyberbezpieczeństwa**, <https://kicb.pl/spoofing-i-vishing-poznaj-ich-tajniki-i-nie-daj-sie-oszustom/>, dostęp 29.05.2022.
- McKinsey & Company**, <https://www.mckinsey.com/pl/our-insights/polska-jako-cyfrowy-challenger>, dostęp 5.05.2022.
- Niebezpiecznik.pl**, <https://niebezpiecznik.pl/post/spoofing-rozmow-telefonicznych/>, dostęp 29.05.2022.
- Niebezpiecznik.pl**, <https://niebezpiecznik.pl/post/cyberalerty-darmowa-aplikacja-od-niebezpiecznika-ostrzegajaca-o-atakach/>, dostęp 23.08.2022.
- Portal KapitanHack.pl**, <https://kapitanhack.pl/2019/01/08/malware/rodzaje-malware-i-sposoby-na-ich-wykrycie-oraz-ochrone/>, dostęp 29.05.2022.
- Profil Zaufany**, <https://pz.gov.pl/pz/index>, dostęp 20.04.2022.
- Serwis informacyjno-usługowy dla przedsiębiorcy**, <https://www.biznes.gov.pl/pl/portal/0074>, dostęp 20.04.2022.
- Serwis informacyjno-usługowy dla przedsiębiorcy**, <https://www.biznes.gov.pl/pl/portal/0075>, dostęp 20.04.2022.
- Serwis Rzeczypospolitej Polskiej**, <https://www.gov.pl/web/gov/uslugi-dla-obywatela>, dostęp 20.04.2022.
- Serwis Rzeczypospolitej Polskiej**, <https://www.gov.pl/web/gov/uslugi-dla-przedsiębiorcy>, dostęp 20.04.2022.
- Serwis Rzeczypospolitej Polskiej**, <https://www.gov.pl/web/gov/uslugi-dla-rolnika>, dostęp 20.04.2022.
- Serwis Rzeczypospolitej Polskiej**, <https://www.gov.pl/web/cyfryzacja/14-milionow-profilu-zaufanych2>, dostęp 5.05.2022.
- Serwis Rzeczypospolitej Polskiej**, <https://www.gov.pl/web/mobywateł>, dostęp 20.04.2022.
- Serwis Sekurak**, <https://sekurak.pl/robak-trojan-wirus-o-co-w-tym-wszystkim-chodzi/>, dostęp 20.04.2022.

Rozwój e-usług w rolniczych ubezpieczeniach społecznych – szanse i zagrożenia

Serwis Sekurak, <https://sekurak.pl/poradnik-o-kluczach-sprzetowych-na-przykladzie-yubikey-5-nfc-2fa-u2f-fido2/>, dostęp 30.05.2022.

Słownik Języka Polskiego, <https://sjp.pwn.pl/slowniki/ONLINE.html>, dostęp 20.04.2022.

System informatyczny Kasy Rolniczego Ubezpieczenia Społecznego, <https://www.ekrus.gov.pl/p4b-web/index.html>, dostęp 20.04.2022.

System informatyczny Kasy Rolniczego Ubezpieczenia Społecznego, <https://www.ekrus.gov.pl/p4b-web/index.html>, dostęp 10.05.2022.

System informatyczny Kasy Rolniczego Ubezpieczenia Społecznego, https://www.ekrus.gov.pl/p4b-web/static/eKRUS_Przewodnik_20220428.pdf, dostęp 10.05.2022.

System informatyczny Kasy Rolniczego Ubezpieczenia Społecznego, <https://www.ekrus.gov.pl/p4b-web/zasadyBezpieczenstwa.html>, dostęp 10.05.2022.

Wikipedia, <https://pl.wikipedia.org/wiki/Internet>, dostęp 20.04.2022.

Zespół CERT Polska, <https://cert.pl/posts/2022/05/krajobraz-bezpieczenstwa-polskiego-internetu-w-2021-roku/>, dostęp 9.05.2022.

Zespół CERT Polska, https://cert.pl/uploads/docs/Raport_CP_2020.pdf, dostęp 9.05.2022.

Zespół CERT Polska, <https://cert.pl/zagrozenia/>, dostęp 29.05.2022.

otrzymano: 26.07.2022
zaakceptowano: 17.10.2022

*Ten artykuł jest objęty licencją Creative Commons Attribution 4.0
Licencja międzynarodowa (CC BY 4.0)*

