



PRAWIDŁOWE KORZYSTANIE Z INTERNETU - BEZPIECZNIE W WIRTUALNYM ŚWIECIE

część 2

MINISTERSTWO
SPRAWIEDLIWOŚCI

www.ms.gov.pl



FUNDUSZ
SPRAWIEDLIWOŚCI

www.funduszsprawiedliwosci.gov.pl



„Sfinansowano ze środków Funduszu Sprawiedliwości, którego dysponentem jest Minister Sprawiedliwości”

Spis treści

Cyberbezpieczeństwo

str. 3

Najczęstsze rodzaje cyberataków

str. 6

Cyberware za naszą wschodnią granicą

str. 10

Skutki działań wojennych

str. 11

Hakerzy grupy Anonymous

str. 12

Cyfrowa Administracja

str. 14

Rozwój i wyzwania

str. 18

Cyberbezpieczeństwo

– definicja i analiza pojęcia

Dla dużej części osób, które stawiają czoło nowym wyzwaniom, jakie spotykają w dzisiejszym skomplikowanym świecie, którego znaczna część przeniosła się do wirtualnej rzeczywistości, zrozumienie pojęcia cyberbezpieczeństwa stało się nieodzowne do bezpiecznego i świadomego funkcjonowania. Należy wziąć pod uwagę, że Internet jest dzisiaj dostępny w każdym miejscu na świecie, koniecznym jest zdefiniowanie pojęcia cyberprzestrzeni, ponieważ to właśnie tam będą stosowane techniki, na których opiera się cyberbezpieczeństwo.

Upraszczając – cyberprzestrzeń jest miejscem wymiany danych i informacji pomiędzy użytkownikami urzędów mających dostęp do Internetu. Dzięki globalnemu charakterowi, co umożliwia wolny dostęp dla każdego zainteresowanego – konieczne jest jedynie łącze internetowe.

Celem zachowania bezpieczeństwa, każdy

– tak jak w życiu codziennym powinien znać techniki korzystania z cyberprzestrzeni. Wspomniana wcześniej globalna dostępność Internetu jest oczywiście tym co stanowi jedną z jego największych zalet, daje bowiem możliwość poznawania innych kultur, wiadomości z najdalszych zakątków globu, czy utrzymywanie relacji z osobami oddalonymi o tysiące kilometrów to niewątpliwie jasne strony tego świata. Cyberbezpieczeństwo jest zatem procesem, którego ideą jest przede wszystkim ochrona danych i systemów wewnętrznych firm, danych osobowych zawartych na nośnikach każdego człowieka przed cyberprzestępcami i ich metodami. Bezpieczeństwo użytkowników sieci rośnie dzięki wdrażaniu nowych odpowiednich technik, procedur, a także dzięki osobom coraz większej liczbie fachowców – informatyków działających w firmach i instytucjach zajmujących się zwiększaniem bezpieczeństwa użytkowników Internetu.





W cyberprzestrzeni nie brakuje kryminalistów upatrujących swojej swoich ofiar, które narażają się na atak swoim nieostrożnym zachowaniem. Cyberprzestępczość wywarła na prawodawcach konieczność stworzenia nowego katalogu czynów zabronionych, a narzędziem lub przedmiotem przestępstwa jest komputer lub inne urządzenia mobilne. Cyberprzestępcy dzięki swoim umiejętnościom technicznym mogą np. do zdobyć dostęp do kont bankowych, dokonywać kradzieży tożsamości, szantażu czy zastraszania. Zazwyczaj są nimi bardzo dobrze wykwalifikowani informatycy, gdyż nie każdy potrafi na takim poziomie korzystać z urządzeń i systemów. Przykładowe działania cyberprzestępców potocznie nazywanych hakerami to: wysyłanie wiadomości e-mail, które wyglądają jak prawdziwe, lecz po ich otwarciu i kliknięciu w zamieszczony link użytkownik traci kontrolę nad swoim urządzeniem a zdalną kontrolę przejmuje cyberprzestępca. Równie częste są też szantaże czy nękanie i upokarzanie w sieci innych osób poprzez gromadzenie i analizę śladów pozostawionych przez ofiary w Internecie.

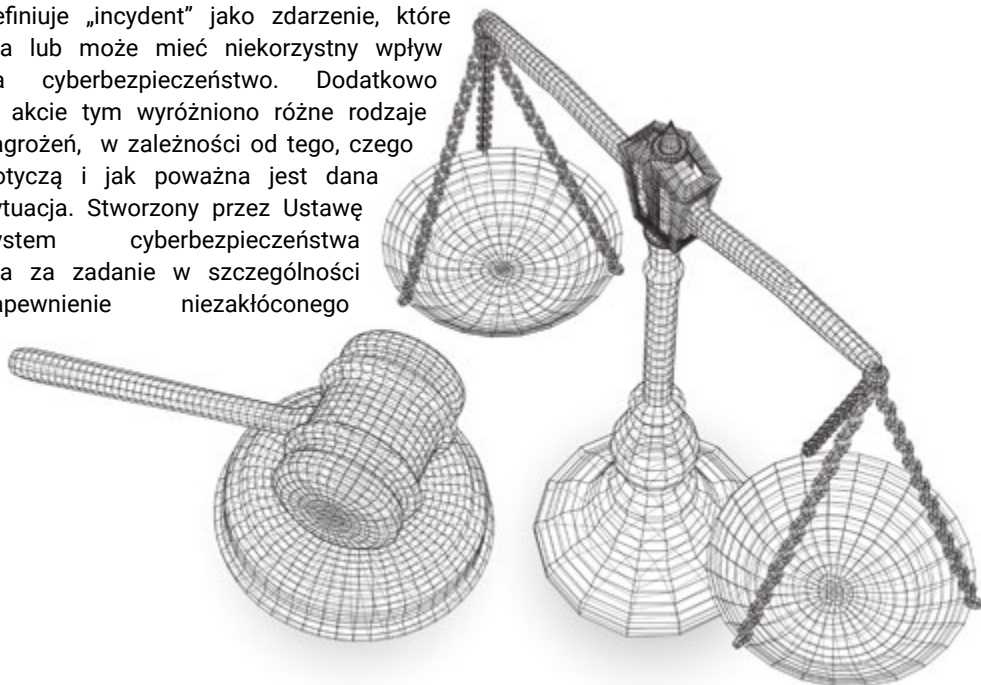
Cennym źródłem informacji dla przestępców w Internecie są np. adresy odwiedzanych stron internetowych czy też informacje zamieszczane w mediach społecznościowych. Głośne były także przypadki ataków na szerszą skalę nazywanych aktami cyberterroryzmu.

Takie działania miały na celu wyrządzenie szkody w odniesieniu do infrastruktury o istotnym znaczeniu dla gospodarki lub obronności atakowanego państwa. Jako przykład takiego ataku można przywołać wydarzenia z 2022 roku, kiedy to portale kilku wojewódzkich komend policji zostały zaatakowane przez rosyjskich hakerów. Mimo iż nie zakłóciło to działań wewnętrznych w atakowanych jednostkach to, ich portale przez dłuższy czas pozostawały niedostępne dla użytkowników. Zatem nie tylko prywatni użytkownicy sieci są narażeni na niebezpieczeństwa w sieci, już wiele lat temu stało się oczywiste, że cyberprzestrzeń stanie się czwartym teatrem dla wojen, które toczą się na świecie.

Obecnie eksperci są zdania, że świat rzeczywisty i wirtualny powinny być jednakowo uregulowane prawnie. W polskim porządku prawnym wyjściem naprzeciw zjawisku informatyzacji świata oddaje decyzja ustawodawcy o wprowadzeniu Ustawy o krajowym systemie cyberbezpieczeństwa z dnia 5 lipca 2018 r. Dokument określa m.in. czym jest krajowy system bezpieczeństwa, ma on na celu zapewnienie cyberbezpieczeństwa na poziomie krajowym. W tej sferze najważniejsze jest niezakłócone świadczenie kluczowych usług cyfrowych, jest to możliwe wyłącznie przez osiągnięcie odpowiedniego poziomu bezpieczeństwa systemów informatycznych. Relacja państwo obywatel, która ma obecnie miejsce także w cyberprzestrzeni musi być maksymalnie bezpieczna dla obu stron. Wspomniana Ustawa o krajowym systemie cyberbezpieczeństwa definiuje „incydent” jako zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo. Dodatkowo w akcie tym wyróżniono różne rodzaje zagrożeń, w zależności od tego, czego dotyczą i jak poważna jest dana sytuacja. Stworzony przez Ustawę system cyberbezpieczeństwa ma za zadanie w szczególności zapewnienie niezakłóconego

świadczenia usług kluczowych i usług cyfrowych oraz osiągnięcie odpowiednio wysokiego poziomu bezpieczeństwa systemów teleinformatycznych służących do świadczenia tych usług.

Powyższe informacje skłaniają do konkretnej refleksji, mianowicie dla poprawy bezpieczeństwa zarówno prywatnych użytkowników sieci jak i państwa, konieczna jest wzmocniona edukacja użytkowników oraz wprowadzanie coraz to nowszych procedur bezpieczeństwa. Ustawodawca nie pozostaje bierny w zakresie edukacji społecznej w tym zakresie, zważając na najważniejszą kwestię – zwrócenie uwagi użytkowników na zagrożenia czające się w cyberprzestrzeni oraz wskazanie skutecznych metod obrony.



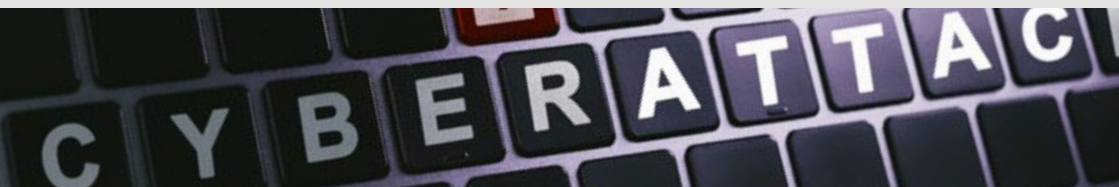
Najczęstsze rodzaje cyberataków

Zdecydowanie, za najbardziej powszechne zagrożenie należy uznać złośliwe oprogramowania, które na różne sposoby mogą znaleźć się na naszych urządzeniach. Często przyczyną zainfekowania danych komputera przez złośliwe oprogramowanie jest nieostrożność samych użytkowników. Pod pojęciem „zainfekowanie” kryją się wszystkie czynności, takie jak np. wirusy czy konie trojańskie, którymi posługują się cyberprzestępcy do wyrządzenia szkody, kradzieży danych oraz przejęcia kontroli nad urządzeniem drugiej osoby.

Skuteczna obrona przed tego typu atakami, jak złośliwe oprogramowanie należy poznać i zrozumieć postacie jakie może ono przybierać. Konieczne jest szczególne wyczulenie użytkowników sieci na wiadomości e-mail otrzymywane od nieznanych nadawców, taka wiadomość może przenosić ładunek wirusa, a po jej otwarciu komputer lub inne urządzenie zostaje zainfekowane.

Konie trojańskie

Należy zachować szczególną ostrożność także przy pobieraniu z pozoru nieszkodliwych aplikacji, potrzebnych nam na co dzień i ułatwiających korzystanie z urządzenia. Niestety, często pod takimi aplikacjami mogą kryć się konie trojańskie, czyli wirusy mogące spowodować awarię zainfekowanego urządzenia, wykraść dane osobowe lub utratę kontroli nad urządzeniem. Są to powszechne i szczególnie niebezpieczne wirusy, przez fakt tego, że jedna część atakującego oprogramowania znajduje się na komputerze zaatakowanym, zaś druga na urządzeniu sprawcy, który może atakować dane wrażliwe, przechwytywać je lub modyfikować. Największym zagrożeniem jest możliwość przechwycenia kontroli nad całym urządzeniem i trwałe jego uszkodzenie. Jest to standardowa technika cyberataku stosowana przez hakerów, niestety usunięcie konia trojańskiego jest szczególnie trudnym zadaniem, do którego należy zatrudniać specjalistów, co generuje dodatkowe koszty.



Scareware

Szczególnie wyrafinowane jest działanie hakerów polegające na wysłaniu nam dwóch komunikatów jednocześnie, pierwszy dot. zainfekowania naszego urządzenia przez wirusa, drugi mówi o możliwości pomocy w związku z tą sytuacją. Dzieje się tak szczególnie przy otwieraniu kolejnych niezasyfrowanych i podejrzanych stron. Paradoks polega na tym, że nasze urządzenie zapewne nie było zainfekowane, a stało się tak dopiero po kliknięciu przycisku pomoc, w komunikacie, który otrzymaliśmy. Takie działanie to właśnie przykład złośliwego oprogramowania, jakim jest tzw. scareware. Opiera się ono na socjotechnice, której celem jest wywołanie u odbiorcy poczucia zagrożenia i paniki oraz niepokoju przed utratą danych. Rzekome działanie wirusa na naszym urządzeniu potęguje stres i powoduje, że zaczynamy działać pod presją, wówczas po kolejnych kliknięciach nieświadomi tego co może się stać zgadzamy się na pierwszą proponowaną opcję pomocy. Skłonienie użytkownika do pobrania oprogramowania oferującego naprawę (nieistniejącego) problemu, kończy się instalacją niepożądanych programów, które w celu skutecznego zakończenia operacji proszą użytkowników o podanie swoich danych osobowych, a niejednokrotnie również kart płatniczych.



Adware

Równie łatwo możemy natknąć się w sieci na tzw. Adware, działanie tego typu złośliwego oprogramowania polega na generowaniu licznych, niepożądanych reklam, czy innych stron internetowych. Często takie reklamy to znane nam z Internetu wyskakujące okna, których treścią są informacje o cudownych dietach, czy sposobach na szybkie wzbogacenie się lub hasła typu „Jemu się udało, jak?”. Okazuje się jednak, że klikając w interesujące hasło czy okno z atrakcyjną treścią wyrażamy zgodę na dostęp do naszej historii wyszukiwania.

Lepszym określeniem Adware niż złośliwe oprogramowanie, jest niedogodność, jest ona jednak równie poważna, ponieważ po przechyceniu naszej historii, może ona być sprzedawana osobom trzecim, np. firmom, które opracowują strategie handlowe lub badają zapotrzebowania rynków zbytu. Takie działania odzierają użytkowników Internetu z prawa do prywatności i możliwości decydowania o udzielaniu informacji.



Uważaj!

Oznakami zainfekowania programami wirusowymi urządzeń mobilnych są, np.: niska wydajność komputera, problemy z uruchamianiem lub zamykaniem urządzenia, przekierowywanie do stron internetowych, których nie mieliśmy zamiaru odwiedzić, ostrzeżenia o atakach wirusowych zawierające również ofertę rozwiązania problemu, czy duża liczba pojawiających się reklam w sieci. Takie okoliczności mogą wzbudzać Twoje uzasadnione podejrzenia, jeśli jednak nie masz odpowiedniej wiedzy i umiejętności, nie podejmuj samodzielnych prób przeciwdziałania im, możesz tylko pogorszyć swoją sytuację.



Specjaliści opracowali już pewne metody, które pomogą Ci zminimalizować, lub całkowicie wykluczyć możliwość zainfekowania urządzeń przez złośliwe oprogramowania.



Oto kilka prostych rad, jak zwiększyć swoje bezpieczeństwo:

- **Podstawą jest aktualizacja oprogramowania urządzenia oraz aplikacji** – gdy tylko są dostępne, ponieważ cyberprzestępcy bazują na niedopracowanych oprogramowaniach stwarzających dla nich luki, które pozwalają na łatwiejsze uzyskanie dostępu.
- **Zwracaj uwagę na liczbę aplikacji zainstalowanych na Twoim urządzeniu.** Instaluj jedynie niezbędne oraz odinstaluj aplikacje, z których już nie korzystasz. Pozwoli to ograniczyć niebezpieczeństwo ataku, np. przez pobranie konia trojańskiego.
- **Jeśli otrzymujesz niespodziewane wiadomości e-mail, w których zawarte są linki z nieznanymi źródeł, ignoruj je.** Jeśli nie klikniesz w link, nic nie powinno się stać.
- **Używaj przeglądarek wyposażonych w systemy do blokowania reklam.** Pomoże Ci to kontrolować pojawiające się treści.

Stosowanie powyższych zasad oraz zwiększanie świadomości o zagrożeniach i specyfice działania złośliwego oprogramowania, pozwoli na bezpieczne korzystanie z sieci oraz uchroni przed atakami cyberprzestępców. Korzystaj z sieci świadomie, to najważniejsza zasada, którą należy się kierować korzystając z dobrodziejstwa Internetu.

Cyberware za naszą wschodnią granicą



Cyberataki są częścią współczesnych działań wojennych. Cyberprzesterzeń stała się nową areną dla konfliktów zbrojnych. Grupy hakerów opłacanych przez rządy, mają możliwości ingerować w systemy teleinformatyczne i oraz zarządzające infrastrukturą krytyczną wrogiego państwa.

W przypadku działań Federacji Rosyjskiej przeciw Ukrainie, ataki cybernetyczne służą demoralizacji i dezinformacji, co ma wpływ na przebieg wojny. W przeddzień inwazji ukraińskie systemy informatyczne oraz agencje i obiekty rządowe, szczególnie w Kijowie zostały sparaliżowane w wyniku cyberataków. Rosyjscy cyberterrorysty wzięli na cel między innymi: siedziby parlamentu, rządu, ministerstwa spraw zagranicznych i innych instytucji państwowych. Ataki były przeprowadzane na serwery internetowe, które były automatycznie zalewane nielegalnymi zapytaniami, co powodowało ich przeciążenie i awarie. Ukraiński rząd oskarżył o te ataki Kreml. Dodatkowe pole walki jakim jest cyberprzestrzeń jest równie niebezpieczne co prawdziwe, po którym jeżdżą czołgi, a nad nim latają samoloty. Wiele systemów infrastruktury obronnej, od przeciwlotniczych, przez raketowe, łączności aż po satelitarne są narażone na wrogie ataki i przejęcia. Cyberprzestrzeń jest nowoczesnym polem walki, chcąc uzyskać przewagę nad przeciwnikiem, albo nawet prowadzić na nim skuteczną cyberobronę konieczne jest zatrudnianie do celów militarnych,

także cywilnych fachowców. Już w pierwszych dniach i tygodniach wojny, na ukraińskich komputerach znajdowane były złośliwe oprogramowania, programy szpiegujące i śledzące oraz wykradające dane wrażliwe. Hakerzy jednej i drugiej strony przechwytywali i zapisywali obrazy z kamer monitoringu, zarówno miejskich, jak i prywatnych, co umożliwiała pozyskiwanie informacji o ruchach wojsk przeciwnika. Ukraina mobilizuje więc nie tylko swoje wojsko, ale także ekspertów z zakresu techniki informatycznej. Rząd ukraiński rekrutuje ochotników - hakerów, którzy będą atakowali rosyjską infrastrukturę wojskową, celem przechwytywania wrażliwych danych i tajnych informacji, ale także dezinformacji przeciwnika. Ukraina otrzymuje również pomoc od ogólnoswiatowego, nieformalnego ruchu hakerskiego „Anonymous”, który ze swojej strony wypowiedział cyfrową wojnę Kremlowi. Do 26 lutego 2022 roku sparaliżowanych zostało szereg stron internetowych rosyjskiego rządu. Podejrzewa się, że stoją za tym aktywiści właśnie z grupy „Anonymous”. Również rosyjski nadawca państwowy rt.com, postrzegany przez Zachód jako narzędzie propagandy Kremla, ucierpiał w wyniku cyberataków. Niezwykle ważną częścią podejmowanych działań przez ukraińskich hakerów jest dokonywanie włamań na kanały rosyjskiej telewizji państwowej i udostępnianie materiałów o zbrodniach na ukraińskich cywilach, czy zwycięstwach ukraińskiej armii.

Skutki działań wojennych

Działania wojenne w cyberprzestrzeni odciskają swoje piętno również w Polsce. Przykładem są media społecznościowe, które zostały zalane falą rosyjskich botów siejących dezinformację. Tysiące negatywnych komentarzy o ukraińskich uchodźcach i negowanie pomocy, jakiej Polska udziela Ukrainie. W związku z dużym zagrożeniem, strategicznie ważnej krajowej i rządowej infrastruktury informatycznej pod koniec maja bieżącego roku premier Mateusz Morawiecki przedłużył obowiązywanie w kraju stopni alarmowych BRAVO i CHARLIE-CRP. Stopień alarmowy CHARLIE-CRP został wprowadzony, aby przeciwdziałać zagrożeniom w cyberprzestrzeni. Po raz pierwszy w Polsce został wprowadzony ten trzeci z czterech stopni alarmowych, premier wprowadził go 21 lutego 2022 roku.

Komisja Nadzoru Finansowego w lutym br. ostrzegła działające w Polsce banki przed możliwością ataków cybernetycznych, za ich prawdopodobną przyczynę podano sytuację za wschodnią granicą RP. Natomiast Resort Obrony Narodowej powołał do funkcjonowania nowy komponent Polskich Sił Zbrojnych - Wojska Obrony Cyberprzestrzeni. Rozwój tego komponentu Polskich Sił Zbrojnych jest konieczny w celu skutecznej obrony i zwiększenia bezpieczeństwa Państwa.



Hakerzy grupy Anonymous



Większość użytkowników urządzeń mobilnych i Internetu spotkała się już niejednokrotnie z licznymi doniesieniami i informacjami na temat działalności hakerów z grupy Anonymous. Grupa składa się z fachowców, którzy swoje ponad normalne zdolności z zakresu informatyki wykorzystują niekoniecznie w dobrym celu. Anonymous są oskarżani o włamania do systemów bankowych, budowanie negatywnej opinii społecznej wobec rządów, a nawet wszczynanie ogromnych manifestacji. Działania jakie podejmują są jednocześnie bardzo głośne i bardzo tajemnicze, kolejne akcje kryją za sobą wiele pytań, które często pozostają bez odpowiedzi. Anonimowi hakerzy najbardziej bronią samej anonimowości, to właśnie ona daje im ochronę i możliwość kontynuowania działań, które zawsze są prowadzone na odległość, z miejsca bezpiecznego, a w wyniku zastosowania własnych technik i zapór systemowych

niezwykle trudno ich wykryć. Pomimo wielu przykładów zagrożeń cybernetycznych, które stwarzała grupa, należy wziąć pod uwagę i podkreślić wspomniane wcześniej działania na rzecz Ukrainy w jej walce z Rosją.

Trudno stwierdzić jak liczna jest to grupa, gdzie mieści się jej baza i czy w ogóle istnieje, czy utrzymują ze sobą kontakt i relacje towarzyskie poza działalnością hakerską. Eksperti z nieukrywanym wstydem wielokrotnie przyznawali, że na temat grupy właściwie więcej nie wiemy niż wiemy. Pewne rzeczy, które jednak udało się ustalić, które grupa o sobie sama ujawniła warto tu przedstawić. Działacze grupy są określanii mianem „haktywistami” – to połączenie słów „haker” i „aktywista”. Nie jest to jednak tylko nazwa grupy, ale ideologia, która stoi u podstaw ich pracy. Hakerzy Legionu twierdzą, że występują przeciw rządowi, wielkim korporacjom, osobom mającym ogromną

władzę i pieniądze. Ich zdaniem podejmują działania w celu obrony najsłabszych – zwykłych ludzi. Dużą część ich pracy stanowi obrona praw obywatelskich, sprzeciw wobec cenzury, konsumpcjonizmowi, niesprawiedliwościom społecznym, dyktaturze. Ich działania polegają oczywiście na dokonywaniu ataków cybernetycznych, które powodują destabilizację rządowych systemów informatycznych i w zamierzeniu mają im odebrać – choćby na chwilę – władzę nad społeczeństwem. Hasłem grupy są słowa: „Obywatele nie powinni bać się swoich rządów. Rządy powinny bać się swoich obywateli”.

Wszyscy utożsamiający się z ideą grupy uważają się za członków Legionu Anonymous, o zasięgu międzynarodowym. Organizacji brak tradycyjnej formalnej i hierarchicznej struktury, brak też w niej jednego, centralnego ośrodka zarządzającego. Składa się na nią szereg mniejszych ugrupowań, ale i pojedynczy aktywiści. Ich głównym środkiem komunikacji jest Internet – media społecznościowe i komunikatory. Także u nas funkcjonuje odnoga pod nazwą AnonPoland/Anonimowi Polska. Do Legionu należy również inna grupa związana z naszym krajem – Squad303. Jej powstanie w Polsce, jest odpowiedzią na rosyjską napaść na Ukrainę, aktualnie zrzesza już hakywistów z całego świata. Przedmiotem działalności grupy jest walka z dezinformacją, którą sieje Kreml oraz rosyjskie służby. Hakerzy z tej polskiej grupy stworzyli i udostępnili m.in. narzędzie, które pozwala wysyłać do losowo wybranych obywateli Rosji SMS-y, które pozwalają podejmować próby przekazywania im prawdziwych informacji o wojnie w Ukrainie. Aplikacja okazała się ważnym narzędziem w walce z kremlofską propagandą – świadczy o tym fakt szybkiej reakcji Rosji, na działania Squad303, która próbowała je bez powodzenia zablokować.

Działalność hakerów wcześniej w pewnej części skupiała się na walce z sektami religijnymi, ugrupowaniami faszystowskimi, nacjonalistycznymi, czy też blokowaniu stron rządów niedemokratycznych i prześladowujących własnych obywateli. Według statystyk hakywiści Anonymous znów zaczęli cieszyć się większą sympatią i uznaniem społecznym, szczególnie w Polsce, która mocno zaangażowała się w pomoc Ukrainie. Powyższe działania na pierwszy rzut oka wydają się szlachetne i godne pochwał, należy jednak pamiętać, że są one podszyte nutą anarchii. Grupa stara się działać na granicy prawa, jednak często je przekracza, a związki z środowiskiem cyberprzestępczym, lub nawet przenikanie przestępców do Anonymous jest jednoznacznie złe.



Cyfrowa Administracja

Historia bardzo przyspieszyła i czasy w których żyjemy są niezwykle dynamiczne. Wojna, czy pandemia koronawirusa wymusiła przyspieszoną transformację cyfrową zmieniając na zawsze model komunikacji i świadczenia usług administracji publicznej. Przeniesienie wielu czynności ze świata rzeczywistego do wirtualnego, wymusza zmiany i dostosowanie możliwości administracji do potrzeb obywateli. Ta sytuacja jest okazją dla rządów i instytucji państwowych, by przemyśleć i ukształtować na nowo swoje strategie nakierowane na długoterminowy i zrównoważony rozwój.

Aktualnym wyzwaniem administracji publicznej jest przejście dynamicznej transformacji, powodowanej presją na stałe podnoszenie sprawności organizacyjnej. Rosną też wymagania i oczekiwania obywateli związane z dostępem do nowoczesnych usług publicznych. Celem cyfryzacji administracji publicznej jest także istotna w dzisiejszych czasach redukcja kosztów i poprawa jakości usług oraz poszerzenie dostępności do informacji publicznych. Konieczne jest stworzenie zintegrowanych usług, jako odpowiedź na realne zapotrzebowanie klientów - obywateli i biznesu.

Korzyści jakie niesie ze sobą Cyfryzacja administracji publicznej:

Wygoda dla obywateli

- Według Diagnozy Społecznej 2013-2014, 65% Polaków deklaruje chęć korzystania z obsługi internetowej w obszarze spraw publicznych.
- Zwiększenie liczby usług dostępnych cyfrowo i ich pełna digitalizacja (end-to-end) wychodzi naprzeciw tym oczekiwaniom.

Szybsze i tańsze procesy

- Zdalne załatwianie spraw to mniejsza czasochłonność zarówno dla obywatela jak i administracji publicznej.
- Cyfryzacja procesów ograniczy ich koszty (np. dzięki internetowym wnioskom zamiast papierowych).



Zwiększenie wpływów podatkowych

- Luka podatkowa VAT szacowana jest na ok. 3% PKB w 2015 r.
- Powrót do sytuacji z 2007 r., kiedy luka ta była najniższa i wynosiła 0,6% PKB, mógłby przynieść budżetowi państwa ponad 42 mld złotych dodatkowych wpływów.

Zmniejszenie szarej strefy

- Według Instytutu Badań nad Gospodarką Rynkową w 2016 roku szara strefa będzie stanowiła w Polsce 19,7% PKB.
- Zwiększenie obrotu bezgotówkowego utrudni działalność w szarej strefie

Nowoczesny wizerunek

- Cyfryzacja i rozwój e-usług publicznych buduje wizerunek nowej, innowacyjnej polskiej gospodarki.
- Nowoczesny wizerunek to promocja polskiej gospodarki oraz szansa na nowe inwestycje

Podnoszenie przejrzystości działania i poziomu bezpieczeństwa.



Równocześnie sektor publiczny mierzy się z wyzwaniami związanymi z dostosowaniem prawa i regulacji do nowych, cyfrowych modeli działania. Musi zapewnić zrównoważone podejście do wdrażania nowych rozwiązań, zapewnić gotowość kadr i społeczeństwa, żeby ograniczyć wykluczenie cyfrowe i zapewnić dostęp do usług publicznych dla wszystkich grup społecznych. Obywatele RP mają do dyspozycji kilkaset usług publicznych, które są udostępnione na różnych platformach, między innymi:

- Elektroniczna Platforma Usług Administracji Publicznej (ePUAP),
- Platforma Usług Elektronicznych Zakładu Ubezpieczeń Społecznych (PUE, ZUS),
- portal obywatel.gov.pl,
- portal biznes.gov.pl.
- dopiero tworzony Portal Rzeczypospolitej Polskiej (Portal RP) – gov.pl, ma on zintegrować witryny internetowe ministerstw, urzędów centralnych i urzędów wojewódzkich oraz ułatwi dostęp do usług cyfrowych, które państwo oferuje obywatelom.



Dostęp do usług publicznych ma każdy, kto może potwierdzić swoją tożsamość w Internecie, np. za pomocą profilu zaufanego (eGO). Profil zaufany także jest bezpłatnym narzędziem, które służy jako elektroniczny podpis w komunikacji z administracją publiczną. Administracja udostępnia, modernizuje oraz buduje nowe e-usługi, które umożliwiają załatwienie spraw urzędowych z dowolnego miejsca i w dowolnym czasie, bez konieczności wychodzenia z domu. Uruchomienie e-usług na różnych portalach zwykle poprzedzone jest procesem logowania do systemu. W wyniku zintegrowania w przyszłości portali tematycznych z Portalem RP, konto elektroniczne gov.pl będzie kluczem do wszystkich cyfrowych usług administracji, co znacznie ułatwi korzystanie z usług administracji. Rozwój e-usług administracji publicznej w Polsce polega głównie na działaniach w kierunku rozwoju cyfryzacji i koncentrują się na kilku obszarach.

Obok rozwoju e-usług należy do nich załączyć:

- tworzenie bardziej przyjaznej legislacji;
- podnoszenie cyfrowych kompetencji społeczeństwa.

Należy wziąć pod uwagę, że w otaczającym nas świecie powszechna staje się informatyzacja życia, również na płaszczyźnie kontaktów z organami państwa i ich wzajemnych relacji. Nie oznacza to jednak utraty stanowisk pracy przez urzędników, a konieczność podnoszenia przez nich kwalifikacji oraz umiejętności informatycznych. Sytuacja związana z procesami wdrażania usług świadczonych elektronicznie nie jest w Polsce najlepsza, szczególnie w urzędach gmin. Problem jest złożony i wynika z wielu przyczyn. Nie zawsze przyczyną takiego stanu rzeczy są problemy budżetowe. Często jest to kwestia wynikająca z organizacji pracy w urzędach i ustalonych priorytetów. Proces pełnej informatyzacji urzędów sektora samorządowego jest niezwykle skomplikowany, szczególnie w zakresie wymiany danych między poszczególnymi szczeblami. Pomiędzy różnymi systemami informatycznymi występują poważne trudności wynikające z braku standaryzacji przesyłanych danych. Platforma oferująca usługi w sposób ujednoczony mogłaby rzucić nowe światło na aspekty świadczenia usług elektronicznych przez jednostki samorządu terytorialnego. Nie będą oni zastępowani przez sztuczną inteligencję, ale wykwalifikowana, nie tylko merytorycznie ale też technicznie kadra urzędnicza pozwoli na bardziej sprawną cyfryzację administracji publicznej. Eksperti wskazują, że państwo musi skoncentrować się na zapewnieniu e-usług adekwatnych do realnych potrzeb, zgłaszanych przez obywateli i przedsiębiorców. Konieczne jest zapewnienie obywatelom możliwości kontaktu z organami administracji publicznej oraz jednostek świadczących usługi publiczne. To najważniejsze zadanie umożliwiające pozyskanie obustronnej relacji o planach, potrzebach i ocenie poszczególnych działań. Administracja musi wsłuchiwać się w głos obywateli, którzy co należy podkreślić – składają się na jej funkcjonowanie płacąc podatki.

Po stronie administracji leży zatem troska o wysoki poziom satysfakcji tak, jak robi to biznes w warunkach konkurencyjnego rynku. Celem rozbudowy systemu E-usług jest upraszczanie obywatelowi życia i odciążanie samych pracowników administracji.

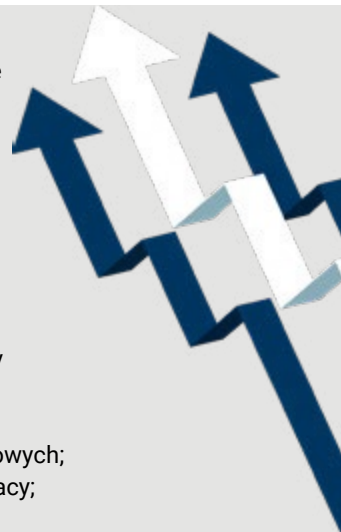


Rozwój i wyzwania

Znaczna część wielu sektorów gospodarki w dynamiczny sposób przechodzi proces cyfryzacji. Zjawisko to zachodzi szczególnie szybko w handlu i usługach, ale także w transporcie, czy przemyśle. Wyraźnie widoczna staje się także automatyzacja oraz masowe przetwarzanie dużej ilości danych. Procesy te pozwalają skrócić czas poświęcany procesom związanym z komunikacją i obiegiem danych. Im więcej ruchów obywatela albo organu w sieci, im większa ilość procesów, tym większe pole do manewru dla cyberprzestępców. Takie okoliczności sprzyjają zwiększaniu ryzyka nadużyć. Phishing, kradzież tożsamości czy podszywanie się pod inne osoby przyczyniły się do powstania ogromnej ilości złośliwego oprogramowania, takiego jak oprogramowanie szantażujące. Nie wymagają żadnych specyficznych uprawnień ani działań po stronie atakowanego – wystarczy zwykła, dobrze znana socjotechnika. Zarówno sposoby działania, jak i narzędzia są uniwersalne i ich używanie jest powtarzane. Nieuchronnie sytuacja ta spowodowała wzrost liczby złośliwych działań w sieci w szczególności prób oszustw internetowych, które mają na celu wykorzystanie obecnego kryzysu. Ogromnym ryzykiem w tym przypadku jest także nadmierne przyspieszona cyfryzacja wymuszona przez pandemię, często realizowana bez wymaganego przygotowania. Z kolei ograniczenia budżetowe sprawiają, że wiele firm nie dysponuje narzędziami, które mogłyby zmniejszyć prawdopodobieństwo i znacząco zredukować skutki ataku. Ogromna ilość podmiotów obecnych na rynku pracy, czy też w obszarze edukacji musiało nagle zmienić charakter pracy i przejść na nauczanie zdalne. To często powodowało przeciążenia serwerów, a na samym początku pandemii brak było konkretnych rozwiązań systemowych, np. w kwestii platform edukacyjnych dla uczniów i studentów.

Chcąc zapobiec zagrożeniu lub podjąć odpowiednie kroki, konieczne jest szybkie działanie nakierowane na wykrycie nietypowej aktywności odpowiednio wcześniej, zanim będzie za późno. Wypracowanie takich standardów i procesów polega na uważnym obserwowaniu operacji wykonywanych na infrastrukturze - zarówno przez człowieka, jak i maszyny. Nietypowe sytuacje, zawsze należy sprawdzić, warto podkreślić kilka podstawowych form działania z wyprzedzeniem:

- śledzenie każdego przypadku zalogowania się użytkownika w nocy lub w weekend;
- sprawdzenie sytuacji, jeśli użytkownik łączy się za pośrednictwem innego niż zwykle lub nieautoryzowanego dostawcy usług internetowych;
- monitorowanie wykorzystania maszyn w godzinach wolnych od pracy;



Podjęcie tych środków, było podyktowane nie przygotowaniem na czas pandemii, który wymusił wirtualizację wielu procesów i zadań, zarówno wykonywanych przez maszyny, jak i przez ludzi. Dotychczasowe zabezpieczenia przestały zapewniać bezpieczeństwo i pełną kontrolę, co często ułatwiało cyberprzestępcom ataki, kradzieże danych itp. W przypadku pracy z danymi wrażliwymi i poufnymi stało się konieczne odpowiednie zabezpieczenie sprzętu z którego pracownicy zaczęli korzystać w domach, przy podłączeniu do słabiej strzeżonych prywatnych sieci WIFI. Najłatwiejszym sposobem na ochronę pracy on-line jest korzystanie z wirtualnej sieci prywatnej (VPN). Usługa VPN tworzy

bezpieczne, zdalne połączenia z innymi sieciami i lokalizacjami geograficznymi. VPN-y zapewniają szereg korzyści każdej firmie. Po pierwsze, zapewniają bezpieczne połączenie nawet wtedy, gdy używamy sieci publicznej Wi-Fi lub sieci prywatnej, która nie jest znana firmie. Ruch sieciowy, niezależnie od tego, czy jest chroniony hasłem, może być podsłuchiwany i wykorzystywany np. do kradzieży tożsamości. Kiedy jednak łączymy się przez VPN, ruch sieciowy jest zaszyfrowany i atakujący będzie wiedział tylko tyle, że dane urządzenie jest podłączone do Wi-Fi. Nie sprawdzi jednak, jakie strony odwiedza użytkownik i co konkretnie robi.



W każdej dziedzinie ludzkiego życia coraz większą część zadań zaczynają spełniać rozwiązania oparte na sztucznej inteligencji. Z jednej strony technologia ta stwarza ogromne korzyści i możliwości, z drugiej – wiąże się z nią ryzyka, którym należy zapobiegać poprzez wdrożenie odpowiednich mechanizmów kontrolnych. W zakresie zgodności z prawem należy mieć na uwadze podejście regulacyjne, w szczególności przygotowywane obecnie w Unii Europejskiej, przepisy. Komisja Europejska stworzyła katalog zakazanych praktyk oraz definicję sztucznej inteligencji. Ogólna zasada zakłada stopniowanie restrykcji zależnie od ryzyka – im większe ryzyko tym bardziej rygorystyczne wymagania. Systemy wysokiego ryzyka objęte będą dodatkowymi obostrzeniami takimi jak: obowiązek sporządzenia szczegółowej dokumentacji, konieczność stosowania odpowiednich praktyk związanych z zarządzaniem danymi, obowiązek dokonywania oceny ryzyka, wymóg rejestrowania zdarzeń czy zapewnienia nadzoru człowieka. Sztuczna inteligencja może przyczynić się do globalnego skoku cywilizacyjnego na miarę czwartej rewolucji przemysłowej.



Z drugiej strony z tą technologią związane są nowe ryzyka np. skłonność do podejmowania decyzji dyskryminacyjnych. Dostrzegając te zagrożenia oraz mając na celu rozwój etycznej sztucznej inteligencji w Europie, Komisja Europejska przygotowała projekt rozporządzenia unijnego, które ma uregulować stosowanie systemów stwarzających najwyższe i wysokie ryzyko. Rozporządzenie to będzie pierwszym unijnym aktem prawnym regulującym sztuczną inteligencję, przy czym akt ten będzie miał wpływ nie tylko na dostawców i użytkowników z Unii Europejskiej, ale również na dostawców i użytkowników z państw trzecich.





Zmiany społeczne i kryzys wywołany pandemią spowoduje niewątpliwie trwałe zmiany w organizacji pracy w każdym z sektorów gospodarki. Praca zdalna prawdopodobnie stanie się w wielu przypadkach standardem, ale zapewne tylko tam gdzie nie będzie przekładało się to na obniżenie efektów pracy. Nowe zagrożenia bezpieczeństwa, jak np. trwająca za naszą wschodnią granicą wojna wymagają reakcji - w tym zwiększonej ochrony systemów informatycznych. Do nie dawna czuliśmy się bezpiecznie, jednak po 24 lutego 2022 r. znaczna część społeczeństwa zrozumiała, że nasze bezpieczeństwo to także odpowiednie zabezpieczenie cyberprzestrzeni. Konieczne jest także budowanie świadomości i organizacja szkoleń dla pracowników oraz ulepszonych technik wykrywania. W tej materii państwo może skutecznie współpracować z podmiotami prywatnymi, jak i wyspecjalizowanymi organizacjami pozarządowymi.

Nowe wyzwanie stoi także przed firmami i dostawcami towarów, którzy muszą stawiać czoła nowym wyzwaniom związanym z cyberbezpieczeństwem.



MINISTERSTWO
SPRAWIEDLIWOŚCI

www.ms.gov.pl



FUNDUSZ
SPRAWIEDLIWOŚCI

www.funduszsprawiedliwosci.gov.pl

„Sfinansowano ze środków Funduszu Sprawiedliwości, którego dysponentem jest Minister Sprawiedliwości”

Broszura powstała w ramach projektu „Bezpieczna Sieć”.