WEI
WARSAW ENTERPRISE INSTITUTE

listopad
2023

SZYMON WITKOWSKI

RAPORT

Poziom bezpieczeństwa cyfrowego Polski

WARSAW ENTERPRISE INSTITUTE

ODPORNI NA CYBERATAKI?

POZIOM BEZPIECZEŃSTWA CYFROWEGO POLSKI

Szymon Witkowski

Radca prawny, magister prawa i administracji, absolwent studiów doktoranckich SGH z zakresu nauk ekonomicznych. Ekspert Związku Przedsiębiorców i Pracodawców przez wiele lat związany z licznymi NGO o profilu wolnorynkowym, środowiskami naukowymi i kulturalnymi. Specjalizuje się w obsłudze prawnej przedsiębiorców. Naukowo koncentruje się na zagadnieniach z pogranicza prawa i ekonomii oraz nowoczesnych technologii. Autor licznych publikacji, raportów i analiz w tym zakresie.

Spis treści

Synteza

- **Polska oceniana jest wysoko pod względem cyberbezpieczeństwa.** W rankingu NCSI zajmujemy bardzo dobrą 11. lokatę, zaś portal Comaritech wśród najbardziej zagrożonych krajów Polskę wymienia na 59. pozycji spośród 75 krajów.
- **W dobie narastających napięć geopolitycznych nikt nie jest bezpieczny. Wraz z rosnącym znaczeniem polityczno-gospodarczym Polski, a także w kontekście napaści Rosji na Ukrainę, rośnie potencjalne zagrożenie atakami cyberprzestępców** zarówno na poziomie publicznych instytucji, jak i indywidualnych obywateli. Mając świadomość znaczenia cyberbezpieczeństwa na szczeblu publicznym np. w Izraelu, na Tajwanie, czy w Estonii, Polska już dziś powinna zwracać uwagę na tego rodzaju zagrożenia i aktywnie się do nich przygotowywać, czerpiąc z gotowych wzorców.
- **Niestety, w ostatnich latach Polsce nie udało się uniknąć kilku spektakularnych wpadek w zakresie cyberbezpieczeństwa.** Dotyczyły one głównie instytucji państwowych i firm obsługujących infrastrukturę krytyczną. Mowa np. o wycieku danych dotyczących polskiego uzbrojenia, wycieku tajnych danych z KPRM, czy o włamaniach do systemów kontroli ruchu pociągów. Należy zaznaczyć, że słabość polskiego systemu może być wykorzystywana przez obce służby wywiadowcze.
- **Również polskie firmy często znajdują się na celowniku hakerów.** Przykładowo atak na CD Projekt Red doprowadził do wycieku całych kodów źródłowych gier tworzonych przez studio, a także wielu krytycznych informacji dotyczących funkcjonowania spółki. Skoro największe firmy mogą paść ofiarą ataków, trudno dziwić się obawom tych należących do sektora MŚP, że nie będą w stanie nadążyć z inwestycjami w środki cyberbezpieczeństwa odpowiednie do zmieniających się czasów.
- **Polscy obywatele korzystają z dobrze zabezpieczonych usług cyfrowych, ale nie są wolni od ryzyka.** Przestępcom trudno jest przeprowadzać „tradycyjne" cyberataki np. na nasze konta bankowe ze względu na ich zaawansowane zabezpieczenia. Zmuszeni są do korzystania z wszelkiego rodzaju metod manipulacji i socjotechniki.
- **Największe wyzwanie dla cyberbezpieczeństwa nie dotyczy procedur, systemów, czy regulacji, a świadomości zagrożeń.** Aż 60 proc. naruszeń systemów ma w sobie element inżynierii społecznej. To właśnie na błędach ludzkich żerują najczęściej przestępcy i to właśnie one najczęściej prowadzą do przełamania systemów bezpieczeństwa.

1. Polska na świeczniku

Wraz ze wzrostem znaczenia gospodarczego Polski rośnie pozycja naszych firm nie tylko w regionie, ale i na świecie. Polskie instytucje, firmy i obywatele coraz częściej będą obierane za cel przez cyberprzestępców.

Polska po odzyskaniu pełnej niezależności przeszła bardzo długą drogę od zacofanego, postsocjalistycznego kraju zmagającego się z problemami transformacji z gospodarki centralnie sterowanej poprzez gospodarkę wolnorynkową o niskim PKB, wysokim bezrobociu i inflacji aż do jednego z liderów regionu, a nawet Europy. Jeszcze w 1989 r. PKB *per capita* Polski wynosiło zaledwie 32,7 proc. niemieckiego[1]. Dla porównania ten sam wskaźnik dla Ukrainy wynosił 43,4 proc., Estonii – 43,2 proc., a dla Węgier – 48,8 proc. Obecnie zgodnie z danymi Eurostatu za 2022 r. Niemcy w stosunku do średniej unijnej posiadają PKB *per capita* na poziomie 117 proc., zaś Polska – 79 proc.[2] Zgodnie z danymi Międzynarodowego Funduszu Walutowego nasz kraj jest 6. największą gospodarką Unii Europejskiej i 22. na świecie[3].

Armia, instytucje publiczne i urzędy mogą stać się celem ataków mających pozyskać informacje tajne i kluczowe dla bezpieczeństwa naszego kraju oraz Sojuszu Północnoatlantyckiego.

Wraz ze wzrostem znaczenia gospodarczego Polski rośnie pozycja naszych firm nie tylko w regionie, ale i na świecie. Rośnie także nasze znaczenie na mapie politycznej, zwłaszcza w kontekście roli, jaką odgrywamy, pomagając Ukrainie w obronie przed inwazją Federacji Rosyjskiej. Nie bez znaczenia są również plany modernizacji naszych sił zbrojnych, które mogą uczynić z naszego kraju najsilniejszą armię w Unii Europejskiej[4] i kluczowego gracza w tej części świata w NATO, co wiązać się będzie z dalszym zacieśnianiem strategicznego sojuszu Polski z USA. Wszystkie te czynniki mogą jednak prowadzić do zwiększania się zagrożeń dla naszego kraju. Będąc „na świeczniku", z pewnością zaczniemy przyciągać uwagę różnych sił dzia-

1 https://zpp.net.pl/wp-content/uploads/2023/07/14.07.2023-Raport-ZPP-1992-2022.-Najlepszy-czas-Polski.pdf, (dostęp na dzień 08.11.2023 r.).
2 https://forsal.pl/gospodarka/pkb/artykuly/8687674,ile-wynosilo-pkb-na-mieszkanca-w-ue-w-2022-r-eurostat-podal-wstepne-wyniki.html, (dostęp na dzień 08.11.2023 r.).
3 https://www.imf.org/en/Publications/WEO/weo-database/2023/April, (dostęp na dzień 08.11.2023 r.).
4 https://www.politico.eu/article/europe-military-superpower-poland-army, (dostęp na dzień 08.11.2023 r.).

łających na świecie. Armia, instytucje publiczne i urzędy mogą stać się celem ataków mających pozyskać informacje tajne i kluczowe dla bezpieczeństwa naszego kraju oraz Sojuszu Północnoatlantyckiego. Polskie firmy mogą stać się celem szpiegostwa korporacyjnego, czy kradzieży własności intelektualnej, danych oraz pieniędzy. Polscy obywatele natomiast, z uwagi na rosnące zarobki, mogą przyciągać uwagę złodziei. O ile jeszcze kilkanaście lat temu kradzież tajnych informacji państwowych, czy korporacyjnych kojarzyła się nam głównie z filmami szpiegowskimi, a kradzież pieniędzy przeciętnego obywatela ze zwykłymi przestępcami, to dziś zjawiska te występują powszechnie w Internecie. To wzrostowi cybernetycznych zagrożeń w naszym kraju postanowiliśmy się przyjrzeć w niniejszym raporcie, aby odpowiedzieć na pytania, czy mamy się czego obawiać, jak wypadamy na tle innych państw i co możemy zrobić, aby się lepiej zabezpieczyć na przyszłość. Na świecie trwają obecnie bardzo intensywne konflikty na cybernetycznym polu walki, którym powinniśmy się przyglądać i zastanowić się, jak możemy przygotować się na podobne scenariusze.

2. Czym jest cyberbezpieczeństwo?

Komisja Europejska oraz agencja ENISA wskazują na osiem najpoważniejszych zagrożeń w tym zakresie: ransomware, malware, zagrożenia socjotechniczne, zagrożenia dostępności sieci, zagrożenia dla danych, dezinformacja, blokada usług, atak na łańcuchy dostaw.

1) Technologie cyfrowe – szanse i zagrożenie

W ciągu ostatnich dziesięcioleci świat przeżywa prawdziwą rewolucję technologiczną. Technologie coraz silniej ingerują w każdą dziedzinę naszego życia, a wraz z pojawieniem się Internetu stały się powszechnym elementem codzienności każdego z nas. Ma to oczywiście niezwykle istotne korzyści. Przede wszystkim jeszcze nigdy świat nie był tak blisko siebie – dziś możemy rozmawiać z każdą osobą, w każdym zakątku świata i wymieniać się informacjami w „czasie rzeczywistym". Mamy dostęp do wszelkich zasobów wiedzy ludzkości, dzięki czemu edukacja stała się powszechna, a rozwój społeczny i technologiczny stale przyspiesza.

Niestety, gwałtowny rozwój technologii cyfrowych wiąże się również z zupełnie nowym rodzajem ryzyka, z którymi musimy się mierzyć. Ryzyka te dotyczą zarówno osób indywidualnych, przedsiębiorstw i instytucji, jak i całych państw. Technologie cyfrowe dają nam niezmierzone możliwości, ale to co jest korzyścią na co dzień, w pewnych warunkach może generować sytuacje zagrażające bezpieczeństwu. Dla przykładu bankowość internetowa zrewolucjonizowała zarządzanie naszymi personalnymi finansami, ale z drugiej strony stworzyła ryzyko nieuprawnionego dostępu do naszych środków osobom, które skutecznie korzystają z luk w systemach zabezpieczeń banku. Kradzież środków z konta może być bardzo dotkliwa dla osoby, która padła ofiarą przestępstwa, ale skala ryzyka jest znacznie większa. We współczesnym świecie systemy informatyczne istnieją przecież w każdej firmie i organizacji, a także służą obsłudze infrastruktury krytycznej. Odpowiadają również za bezpieczeństwo ruchu drogowego, wodnego, czy lotniczego w wielu państwach. Są one także obecne bezpośrednio w obronności i wojskowości. Trudno zatem przecenić ryzyko naruszenia tego rodzaju systemów we wszelkiego rodzaju atakach hybrydowych i terrorystycznych.

Systemy informatyczne, które służą nam na co dzień są narażone na różnego rodzaju zagrożenia, a ochrona przed nimi określana jest zbiorczo jako cyberbezpieczeństwo. W powszechnym

użyciu używa się różnych definicji tego zjawiska, np. amerykańska agencja CISA zajmująca się tym tematem podaje, że:

Cyberbezpieczeństwo to sztuka ochrony sieci, urządzeń i danych przed nieautoryzowanym dostępem lub wykorzystaniem w celach przestępczych oraz praktyka zapewniania poufności, integralności i dostępności informacji[5].

Słownik Cambridge podaje z kolei, że:

Cyberbezpieczeństwem są działania podejmowane w celu ochrony osoby, organizacji lub kraju oraz ich informacji komputerowych przed przestępstwami lub atakami przeprowadzanymi za pośrednictwem Internetu[6].

Wreszcie EY Polska na swojej stronie internetowej posługuje się następującą definicją:

Cyberbezpieczeństwo to ochrona danych i systemów wewnętrznych przed zagrożeniami, jakie niosą za sobą cyberataki. W takiej definicji mieści się nie tylko technologia, lecz także cały proces, który kontroluje i ochrania sieć, programy i urządzenia. Najważniejszym celem zapewnienia bezpieczeństwa w sieci jest zmniejszenie ryzyka ataków cybernetycznych oraz skuteczna ochrona przed nieuprawnionym wykorzystaniem danych i programów[7].

5 https://www.cisa.gov/news-events/news/what-cybersecurity, (dostęp na dzień 08.11.2023 r.).
6 https://dictionary.cambridge.org/dictionary/english/cybersecurity, (dostęp na dzień 08.11.2023 r.).
7 https://www.ey.com/pl_pl/cybersecurity/cyberbezpieczenstwo-jak-zadbac-o-bezpieczenstwo-w-sieci, (dostęp na dzień 08.11.2023 r.).

2) Rodzaje zagrożeń w sieci

Mając świadomość tego, czym jest cyberbezpieczeństwo i jak ważne jest ono dla całego społeczeństwa we współczesnych czasach, należy ustalić, jakie są najważniejsze źródła zagrożeń dla systemów informatycznych. Komisja Europejska oraz agencja ENISA wskazują na 8 najpoważniejszych zagrożeń w tym zakresie[8]. Warto zapoznać się z tymi pojęciami dla lepszego zrozumienia niebezpieczeństw opisanych w dalszych częściach raportu.

[8] https://www.europarl.europa.eu/news/en/headlines/society/20220120STO21428/cybersecurity-main-and-emerging-threats?&at_campaign=20234, (dostęp na dzień 08.11.2023 r.); ENISA Threat Landscape 2022.

Ransomware

W atakach tego rodzaju hakerzy przejmują kontrolę nad czyimiś danymi i żądają okupu za przywrócenie do nich dostępu. Słowo to pochodzi od zbitki słów „ransom" – okup i „software" – oprogramowanie. Atak następuje za pomocą złośliwego oprogramowania, przeważnie tak zwanego „konia trojańskiego". Późniejszy dostęp do danych przez prawowitego użytkownika może być utrudniony (blokadę może zdjąć specjalista w serwisie) bądź niemal niemożliwy (w przypadku zastosowania zaawansowanego złośliwego oprogramowania). Ten rodzaj ataku na system informatyczny przebiega poprzez wykorzystanie luki w usłudze sieciowej (w wyniku stosowania np. niewystarczających zabezpieczeń) bądź błędu samego człowieka.

Historia ataków ransomware jest bardzo długa, pierwszym znanym tego rodzaju złośliwym oprogramowaniem był „AIDS", napisany w 1989 r. przez Josepha Poppa, który ukrywał dane na dysku użytkownika, informując, że licencja na korzystanie z tych plików wygasła i żądając wpłaty 189 dolarów w celu ich odblokowania.

Według EINSA w 2022 r. ataki ransomware, podobnie jak w latach poprzednich, były jednym z głównych cyberzagrożeń. Wyniki badania przeprowadzonego pod koniec 2021 r. i w 2022 r. wskazują, że ponad połowa respondentów lub ich pracowników padła ofiarą ataków ransomware. Szacuje się, że w 2021 r. globalne szkody wyrządzone przez oprogramowanie ransomware osiągnęły wartość 18 mld euro – 57 razy więcej niż w 2015 r.

Malware

Malware (od „malicious" – „złośliwy" i „software" – oprogramowanie) to złośliwe oprogramowanie, które uszkadza system bądź wpływa w sposób niepożądany na jego działanie. Należą do niego różnego rodzaju wirusy, robaki, programy szpiegujące czy konie trojańskie.

Jest to ogólna kategoria zagrożenia wskazana przez ENSA z uwagi na powszechność występowania różnego rodzaju złośliwego oprogramowania w sieci. Agencja wskazuje, że po globalnym spadku ilości tego rodzaju programów w czasie pandemii COVID-19 w 2020 i 2021 r., jego wykorzystanie wzrosło znacząco pod koniec 2021 r., gdy ludzie zaczęli wracać do biur. Wskazuje to pośrednio, że programy tego rodzaju często są nakierowane na infekowanie komputerów służbowych w organizacjach z wykorzystaniem błędów ludzkich.

EINSA wskazuje też, że wzrost liczby malware związany jest ze wzrostem popularności zjawiska crypto-jackingu, czyli potajemnego i nielegalnego wykorzystania komputera ofiary do kopania kryptowalut. Kolejną przyczynę wzrostu ilości tego rodzaju programów upatruje się w atakach na systemy „Internetu Rzeczy", czyli np. „inteligentne domy". W takim przypadku niepowołana osoba może uzyskać dostęp np. do kamery w naszym mieszkaniu. Agencja wskazuje, że zaledwie w ciągu pierwszych sześciu miesięcy 2022 r. odnotowano więcej tego rodzaju ataków, niż w ciągu poprzednich czterech lat łącznie.

Zagrożenia socjotechniczne/inżynieria społeczna

Zagrożenia tego rodzaju koncentrują się na wykorzystaniu błędów ludzkich do naruszenia systemów bezpieczeństwa. Polegają one na nakłanianiu ofiar do otwierania złośliwych plików, wiadomości mailowych, wchodzenia na zainfekowane strony internetowe itp. W ten sposób użytkownik nieświadomie instaluje na swoim urządzeniu złośliwe oprogramowanie bądź podaje wrażliwe dane mogące służyć do kradzieży tożsamości. Najczęstszym atakami tego rodzaju jest phising, czyli podszywanie się pod inną osobę czy instytucję w wiadomości e-mail w celu wyłudzenia danych, np. dostępu do konta bankowego bądź nakłanianie do pobrania zainfekowanego pliku. Często przestępcy wysyłają wiadomość, korzystając z domeny i strony do złudzenia przypominającej nasz bank, prosząc np. o zalogowanie do bankowości internetowej. **Według badań cytowanych przez ENISA, niemal 60 proc. naruszeń w Europie, na Bliskim Wschodzie i w Afryce zawiera element inżynierii społecznej.**

Zagrożenia dla danych

Zagrożenia polegające na uzyskaniu nieuprawnionego dostępu do danych i możliwość ich ujawnienia są niezwykle powszechne i niebezpieczne we współczesnej gospodarce. Dla wielu firm bezpieczeństwo danych jest kwestią podstawową. Dane mogą zawierać kluczowe kwestie dotyczące technologii, procesów i mogą stanowić o przewadze konkurencyjnej przedsiębiorstw. Zagrożenia w tym zakresie mogą dotyczyć zarówno celowych ataków na systemy bezpieczeństwa, jak i wycieku danych. ENISA wskazuje, że głównym motywem działalności cyberprzestępców jest chęć zarobku, ale w około 10 proc. przypadków jest nim szpiegostwo.

Denial of Services

Zagrożenia dotyczące dostępności do usługi również są jednymi z najbardziej powszechnych. Obecnie ataki mają charakter Distributed Denial of Services (DDoS), czyli prowadzone są z wielu miejsc/urządzeń jednocześnie. Powodują one brak możliwości skorzystania z określonych systemów bądź całej infrastruktury. Dotykają zarówno sieci mobilnych, jak i podłączonych do nich urządzeń. Obecnie rośnie ich popularność jako środków wykorzystywanych w tak zwanych działaniach hybrydowych np. w cybernetycznej wojnie rosyjsko-ukraińskiej, w konflikcie izraelsko-palestyńskim, czy w chińskich atakach na Tajwan.

Zagrożenia dostępności do Internetu

W przeciwieństwie do ataków Denial of Services, w tym przypadku celem jest uniemożliwienie użytkownikom dostępu do samej sieci, najczęściej poprzez przejęcie lub zniszczenie infrastruktury. Tego rodzaju działania są obserwowane w trakcie trwającej wojny rosyjsko-ukraińskiej.

Dezinformacja

Jest to zagrożenie, które połączone jest ze wzrostem popularności wszelkiego rodzaju mediów społecznościowych. Często są one wykorzystywane w kampaniach rozpowszechniających dezinformację (celowo sfałszowane informacje), jak i rozpowszechniających błędne informacje. Często tego rodzaju działania mają na celu szerzenie strachu i niepewności. Są powszechnie stosowane choćby w „wojnie cybernetycznej" i mają obecnie bardzo duże znaczenie.

Ataki na łańcuchy dostaw

Jest to atak mający na celu zaburzenie relacji i współpracy między dostawcami i odbiorcami. Polega między innymi na podważeniu wzajemnego zaufania między stronami i może być niezwykle niebezpieczny dla światowego obrotu gospodarczego.

Z badań przeprowadzonych przez Europejską Agencję do spraw Cyberbezpieczeństwa wynika, że w Unii Europejskiej na powyższe zagrożenia najbardziej narażone są następujące podmioty (procentowy udział w ogóle zdarzeń dotyczących naruszenia cyberbezpieczeństwa):

- Administracja publiczna/rząd (24 proc. zgłoszonych incydentów),
- Dostawcy usług cyfrowych (13 proc.),
- Osoby indywidualne/ogół społeczeństwa (12 proc.),
- Usługi (12 proc.),
- Finanse/bankowość (9 proc.),
- Zdrowie (7 proc.)[9].

[9] https://www.europarl.europa.eu/news/en/headlines/society/20220120STO21428/cybersecurity-main-and-emerging-threats?&at_campaign=20234, (dostęp na dzień 08.11.2023 r.).

3. Cyberbezpieczeństwo w Polsce i na świecie – osoby fizyczne, organizacje i państwo

- **Informacje o naruszeniach cyberbezpieczeństwa w kontekście osób fizycznych w Polsce zbiera choćby CERT Polska, który w 2022 r. zarejestrował 39 683 incydenty cyberbezpieczeństwa. To 34-procentowy wzrost w stosunku do ubiegłego roku.**
- **Polska znajduje się w gronie najczęściej atakowanych cybernetycznie państw w Europie. Przykładowo przeciętna polska organizacja (taka, jak przedsiębiorstwo) była w czerwcu 2022 r. atakowana średnio 938 razy.**
- **Obecnie Polska nie należy do ścisłej czołówki najczęściej atakowanych państw. Ten „przywilej" zgodnie z danymi BlackBerry należy kolejno do Stanów Zjednoczonych (aż 65 proc. ataków), Japonii (8 proc.), Brazylii (6 proc.), Kanady (5 proc.), czy Australii i Meksyku (po 4 proc.)[10].**

Rosnąca rola gospodarcza i polityczna Polski wiąże się z rosnącym zagrożeniem cybernetycznym. Ponieważ istnieje zależność między stopniem rozwoju gospodarczego a rolą systemów informatycznych w danym kraju, z pewnością Polska jest w gronie państw, w których bezpieczeństwo cybernetyczne pełni szczególnie ważną funkcję, która z czasem będzie się jedynie zwiększała. Kwestii tej z pewnością należy przyjrzeć się zarówno z perspektywy przeciętnego obywatela, jak i organizacji (głównie przedsiębiorstw) oraz całego państwa.

1) Osoby fizyczne

Z całą pewnością indywidualni użytkownicy są najpowszechniejszą grupą korzystającą z sieci, a tym samym są narażeni na najbardziej zróżnicowane zagrożenia, które mogą wpłynąć na ich osobistą sytuację. Praktycznie niemożliwe jest dokładne oszacowanie ilości niebezpiecznych zdarzeń i incydentów w tej grupie podmiotów. Niemniej jednak warto posłużyć się dostępnymi danymi z zastrzeżeniem, że faktyczna ilość incydentów z pewnością jest znacznie większa. Informacje o naruszeniach cyberbezpieczeństwa w Polsce zbiera choćby CERT Polska, który w 2022 r. wytypował 115 164 zgłoszenia, z których zarejestrował 39 683 incydenty cyberbezpieczeństwa. To 34-procentowy wzrost w stosunku do

[10] https://www.blackberry.com/content/dam/bbcomv4/global/pdf/0408-Threat-ReportV17.pdf, (dostęp na dzień 08.11.2023 r.).

ubiegłego roku. Najczęściej zgłaszanymi problemami były oszustwa komputerowe, szczególnie phishing. Aż 64 proc. (25 645 przypadków) incydentów zarejestrowanych przez CERT Polska stanowił właśnie ten rodzaj zagrożenia. Samych zgłoszeń dokonanych przez internautów było 82 830. Najpopularniejszymi rodzajami phishingu było podszywanie się pod znane marki działające na polskim rynku – InPost, Dacebook i Vinted. Drugim najpopularniejszym zagrożeniem, zdaniem CERT Polska, było szkodliwe oprogramowanie (15 433 zgłoszenia i 3409 incydentów), zaś trzecim włamania do systemów informatycznych i kont pocztowych[11].

Skalę zagrożeń dla polskich internautów prezentuje również badanie przeprowadzone przez serwis ChronPESEL.pl i Krajowy Rejestr Długów, które wskazuje, że 15 proc. Polaków padło ofiarą, a aż 40 proc. doświadczyło próby wyłudzenia danych osobowych. Ponadto 21 proc. ankietowanych nie jest w stanie stwierdzić, czy do takiego wycieku w ich przypadku nie doszło. 60 proc. ankietowanych Polaków wskazuje, że obawiają się kradzieży danych osobowych. Jako największe zagrożenie ankietowani wskazywali możliwość włamania hakerów do komputera lub telefonu (60 proc.), phishing (57 proc.), wycieki z baz danych (52 proc.) oraz fizyczną kradzież dokumentów (48 proc.)[12]. Należy podkreślić, że obawy o bezpieczeństwo danych osobowych nie są bezpodstawne. Utrata danych osobowych może narazić nas na szereg bardzo nieprzyjemnych konsekwencji. Jednym z „łagodniejszych" skutków wycieku danych może być pojawienie się naszego nr telefonu, czy adresu e-mail w różnego rodzaju bazach danych wykorzystywanych na potrzeby marketingowe bez naszej zgody. Czasem te same dane mogą posłużyć jako furtka do kolejnych prób uzyskania bardziej wrażliwych informacji np. danych dostępowych do konta bankowego przez phishing. Wyciek bardziej wrażliwych danych może prowadzić nawet do możliwości zaciągania zobowiązań przez przestępców na nasze konto bez naszej wiedzy. W takiej sytuacji o całej sprawie możemy dowiedzieć się od komornika, który będzie podejmował próby egzekucji zaległych zobowiązań np. z niespłacanej pożyczki, którą „na nasze konto" zaciągnęli przestępcy. Taka sytuacja jest nie tylko bardzo stresująca, ale również bardzo problematyczna prawnie, gdyż podważenie legalności zaciągniętych zobowiązań i uwolnienie się od odpowiedzialności w takim przypadku jest często niełatwe, czasochłonne i kosztowne.

Posłużmy się jednym z najpowszechniejszych przypadków wyłudzenia danych, na który w ostatnich latach narażeni są Polacy – telefonów od osób podszywających się za przedstawicieli banku. Oszuści często w takiej sytuacji są odpowiednio przygotowani, możliwe, że na skutek wcześniejszego wycieku wiedzą, że ich potencjalna ofiara posiada rachunek w konkretnym banku, jak się nazywa, jaki ma nr PESEL i jaki posiada numer telefonu. Dane te jednak nie wystarczą do dokonania włamania, konieczne jest pozyskanie innych informacji po to, aby przejść proces weryfikacji w banku. Sposób, w jaki działają przestępcy opisuje między innymi Federacja Rozwoju Rynku Finansowego[13]. Korzystając z zabiegów socjotechnicznych, podszywają się oni pod pracownika banku i kontaktują się z potencjalną ofiarą, „ostrzegając" ją przed próbą wyłudzenia pożyczki na ich nazwisko. Przeważnie osoba, która odebrała taki telefon, jest zaskoczona, zaniepokojona sytuacją i niejednokrotnie poddaje się manipulacji.

Obawy o bezpieczeństwo danych osobowych nie są bezpodstawne. Utrata danych osobowych może narazić nas na szereg bardzo nieprzyjemnych konsekwencji.

[11] Roczny raport z działalności CERT POLSKA 2022, Krajobraz bezpieczeństwa polskiego Internetu, https://cert.pl/uploads/docs/Raport_CP_2022.pdf, (dostęp na dzień 08.11.2023 r.).

[12] https://chronpesel.pl/aktualnosci/dzien-ochrony-danych-osobowych-2023, (dostęp na dzień 08.11.2023 r.).

[13] https://frrf.pl/telefoniczni-oszusci-nie-odpoczywaja-tym-razem-probuja-ostrzec-przed-wyludzeniem-kredytu, (dostęp na dzień 08.11.2023 r.).

Przestępca może nakłonić taką osobę do podania danych niezbędnych do przejęcia dostępu do konta i wyprowadzenia środków, czy zawarcia umowy pożyczki. Popularną wersją takiego oszustwa jest również nakłonienie potencjalnej ofiary przestępstwa do dokonania przelewu środków „na bezpieczne konto", aby ustrzec się przed włamaniem. Doniesień medialnych o tego rodzaju zdarzeniach jest bardzo dużo, np. lubelska „Gazeta Wyborcza" opisuje przypadek, gdy 44-latka straciła 35 tysięcy złotych, gdyż uwierzyła oszustce podszywającej się za pracownicę banku, że ktoś chce wziąć kredyt na jej dane[14]. Co gorsza, okazuje się, że nawet bez tego rodzaju telefonów oszuści są w stanie zaciągnąć zobowiązania w instytucjach pożyczkowych bez naszej wiedzy, dysponując odpowiednio kompletnymi danymi pochodzącymi z wycieku.

Podkreślić jednak należy, że pomimo licznych niebezpieczeństw, na które narażeni są użytkownicy nowoczesnych usług finansowych, to w praktyce do naruszenia systemów bezpieczeństwa banków i innych instytucji finansowych dochodzi na skutek błędu ludzkiego. Przestępcy zmuszeni są do korzystania z socjotechniki i manipulują osobami, które chcą oszukać, gdyż tylko w ten sposób są w stanie przejść zabezpieczenia bankowe. Polska wskazywana jest od lat jako jeden z liderów nowoczesnej bankowości, która siłą rzeczy przekłada się na bezpieczeństwo systemów bankowych. Polskie banki wymieniane były w gronie najnowocześniejszych zarówno w badaniach[15], jak i są doceniane przez największe instytucje bankowe świata[16] oraz otrzymują liczne nagrody jak np. zdobycie pierwszego miejsca przez PKO BP w rankingu Finnoscore 2023[17]. Z całą pewnością należy w tym miejscu podkreślić, że nawet najlepsze zabezpieczenia natury technicznej nie są w stanie ochronić systemów informatycznych przed błędem ludzkim, dlatego niezwykle ważne jest stałe zwiększanie świadomości użytkowników o zagrożeniach i o sposobach, by się przed nimi ustrzec.

Oczywiście Polska nie jest w tym zakresie wyjątkiem. Podobne przestępstwa do wskazanych powyżej popełniane są na całym świecie. Jak podaje amerykańskie biuro Federal Trade Commision w 2022 r. konsumenci stracili blisko 8,8 miliarda dolarów na skutek oszustw, z czego 2,6 miliarda w wyniku wyłudzenia danych przez osoby podszywające się np. pod pracowników banków. Amerykańskie media ostrzegają obywateli o działalności tak zwanych „Fantomowych Hackerów", którzy działają analogicznie do przestępców w Polsce[18].

Na koniec warto wspomnieć o rozwijających się trendach w zakresie przestępczości cybernetycznej[19]. Liczne organizacje ostrzegają o wykorzystaniu przez hakerów rosnącej popularności Internetu Rzeczy, a więc np. systemów inteligentnych domów. Znajdując lukę w zabezpieczeniach, mogą oni np. uzyskać dostęp do kamer monitoringu w naszej nieruchomości, zbierając potrzebne im informacje o tym, co posiadamy i gdzie się to znajduje oraz kiedy jesteśmy w domu. Włamanie do systemu pomaga im pokonać wszelkiego rodzaju zabezpieczenia, w tym alarmy. Prawdziwi włamywacze paradoksalnie w takich sytuacjach mogą mieć bardzo ułatwione zadanie. O popularności tego rodzaju przestępstw informują media szczególnie w tych krajach, w których inteligentne domy zyskały już sporą popularność, jak np. w USA[20].

---

14 https://lublin.wyborcza.pl/lublin/7,48724,29845541,uwierzyla-oszustce-ze-ktos-chce-zaciagnac-kredyt-na-jej-dane.html, (dostęp na dzień 08.11.2023 r.).

15 Deloitte, *CE Banking Outlook Winning in the Digital Arms Race,* October 2016, https://www2.deloitte.com/content/dam/Deloitte/ro/Documents/about-deloitte/CE-Banking-Outlook.pdf, (dostęp na dzień 08.11.2023 r.).

16 https://www.casfera.pl/polska-swiatowym-liderem-w-bankowosci-elektronicznej, (dostęp na dzień 08.11.2023 r.).

17 https://media.pkobp.pl/246016-pko-bank-polski-europejskim-liderem-cyfrowej-bankowosci, (dostęp na dzień 08.11.2023 r.).

18 https://www.livenowfox.com/news/watch-out-phantom-hacker-scams-fbi-warns, (dostęp na dzień 08.11.2023 r.).

19 https://aag-it.com/the-latest-cyber-crime-statistics, (dostęp na dzień 08.11.2023 r.).

20 https://www.foxnews.com/tech/digital-burglaries-threat-your-smart-home-devices; https://nypost.com/2018/12/12/your-smart-devices-might-make-it-easier-for-burglars-to-break-in, (dostęp na dzień 08.11.2023 r.).

2) Organizacje

Pod pojęciem organizacji w niniejszym opracowaniu rozumiemy podmioty zorganizowane, głównie przedsiębiorstwa, ale też firmy będące prowadzone przed osoby fizyczne, a także inne instytucje niebędące kontrolowane bezpośrednio przez państwo i jego organy. Z całą pewnością jest to grono podmiotów przyciągające uwagę przestępców zarówno z uwagi na względy finansowe, jak również z powodu szpiegostwa gospodarczego. W 2022 r. portal dziennik.pl powołując się na badania Check Point Research, wskazywał, że Polska znajduje się w gronie najczęściej atakowanych cybernetycznie państw w Europie, a przeciętne polska organizacja była w czerwcu 2022 r. atakowana średnio 938 razy. Zdecydowanie najczęściej atakowano podmioty sektora finansowego (1100 ataków tygodniowo), rządowego i wojskowego (1047 ataków) oraz infrastruktury (681 ataków). Przy czym podkreśla się, że są to statystyki zbliżone do globalnych, natomiast w Polsce przedmiotem zainteresowania cyberprzestępców znacznie rzadziej jest np. edukacja[21].

W podobnym tonie wypowiada się Cyberark w swoim raporcie. Zgodnie z przedstawionymi danymi 89 proc. organizacji padło ofiarą ataku typu ransomware w ostatnich 12 miesiącach. Aż 93 proc. podmiotów obawia się, że rozwój narzędzi AI przyczyni się do pogorszenia się cyberbezpieczeństwa w 2023 r. Ponadto 74 proc. badanych wskazuje, że ich organizacja jest zaniepokojona możliwością utraty danych z powodu błędu pracowników, byłych pracowników oraz współpracowników. Raport jednoznacznie podkreśla, że to właśnie błędy ludzkie są największym problemem systemów bezpieczeństwa[22].

Aż 93 proc. podmiotów obawia się, że rozwój narzędzi AI przyczyni się do pogorszenia się cyberbezpieczeństwa w 2023 roku.

Niepokojące informacje płyną także z danych dostarczonych przez jednego z liderów oprogramowania antywirusowego i zabezpieczeń komputerowych – firmy ESET. Wskazuje ona, że ponad dwie trzecie z firm z sektora MŚP biorących udział w ich badaniu wskazywało, że doświadczyło incydentu związanego z bezpieczeństwem IT. Średni szacunkowy koszt takiego zdarzenia to 220 000 euro, a więc ponad milion złotych. Wśród polskich przedsiębiorców odsetek tych, które doświadczyły ataku, był nieco mniejszy i wyniósł 59 proc. Rodzime firmy wskazują, że największe zagrożenia dla cyberbezpieczeństwa płyną z braku świadomości pracowników oraz ograniczeń budżetowych. Niska świadomość cyberzagrożeń wśród kadr była wskazywana przez aż 94 proc. polskich ankietowanych i 84 proc. całej grupy. Ogół respondentów wskazuje, że najbardziej obawia się przede wszystkim utraty danych, konsekwencji finansowych ataków oraz utraty zaufania partnerów biznesowych. ESET przedstawia także główne zagrożenia, z jakimi spotkały się firmy z sektora MŚP, którymi są:

- Złośliwe oprogramowanie (70 proc.),
- Ataki na strony internetowe (67 proc.),
- Ransomware (65 proc.),
- Problemy bezpieczeństwa stron trzecich (64 proc.),
- Ataki typu DDoS (60 proc.),
- Ataki typu Remote Desktop Protocol (60 proc.).

Co istotne, polskie firmy biorące udział w badaniu wskazywały, że obawiają się kosztów inwestycji w cyberbezpieczeństwo oraz że nie będą w stanie dotrzymać kroku rozwojowi technologii w zakresie cyberbezpieczeństwa[23]. O ile zatem polskie firmy nie są częściej atakowane niż przeciętne przedsiębiorstwa na świecie, to z całą pewnością

[21] https://technologia.dziennik.pl/internet/artykuly/8480634,hakerzy-ataki-europa-check-point.html, (dostęp na dzień 08.11.2023 r.).
[22] Cyberark, 2023 Identity Security Threat Landscape Report.
[23] https://www.eset.com/pl/about/newsroom/press-releases/news/cyberzagrozenia-polskie-firmy-nie-czuja-sie-bezpiecznie, (dostęp na dzień 08.11.2023 r.).

za niepokojące można uznać to, że ich kondycja finansowa może utrudnić wprowadzanie nowatorskich rozwiązań, co w konsekwencji może powodować większą ilość luk w systemach bezpieczeństwa w Polsce, niż w bogatszych krajach UE i świata. Pośrednio jest to również efekt trudnej sytuacji gospodarczej rodzimych firm na przestrzeni ostatnich lat, rosnących kosztów działalności, niestabilności prawa, zerwania łańcuchów dostaw, pandemii COVID-19, czy wojny u naszego wschodniego sąsiada – Ukrainy. W tych realiach trudno jest firmom realizować inwestycje, również te w zakresie bezpieczeństwa cybernetycznego.

O bezpieczeństwie informatycznym polskich przedsiębiorców pisał także portal gazety „Dziennik Gazeta Prawna", który wskazuje, że Polska jest szczególnie częstym celem ataków hakerskich z uwagi na fakt, iż jest krajem frontowym. Podkreśla, że w dzisiejszych czasach sam antywirus nie jest wystarczający i należy rozważyć bardziej zaawansowane formy ochrony komputerów w firmach. Wskazuje także, że pomocne w utrzymaniu bezpieczeństwa może być przyjrzenie się regulacjom dotyczącym bezpieczeństwa danych, którym podlegają pracownicy zdalni. Poza siedzibą pracodawcy trudno jest mu bowiem kontrolować zachowania swoich pracowników, a korzystanie z otwartych sieci, pozostawianie sprzętu służbowego bez nadzoru, czy korzystanie z tego sprzętu w celach prywatnych przez pracowników często naraża firmę na poważne niebezpieczeństwo cyfrowe[24].

O tym, jak poważne mogą być konsekwencje ataków przestępców na systemy informatyczne firm, może świadczyć przykład CD Projekt Red. W lutym 2021 r. hakerzy włamali się do systemów firmy i wykradli szereg wrażliwych danych, w tym kody źródłowe produkcji (gier) studia. Przestępcy zażądali okupu w zamian za nieupublicznianie tych danych, na co jednak studio się nie zgodziło. Efektem było upublicznienie w sieci niektórych kodów źródłowych. Nie jest w pełni wiadome, ile ważnych danych trafiło na „czarny rynek". Istnieje ryzyko, że w rękach nieupoważnionych osób znalazły się także dokumenty prawne, księgowe, administracyjne, HR i dotyczące relacji inwestor-

[24] https://serwisy.gazetaprawna.pl/nowe-technologie/artykuly/8693810,jak-zabezpieczyc-firme-przed-cyberatakami.html, (dostęp na dzień 08.11.2023 r.).

skich. Spółka przyznała, że wśród wykradzionych danych mogły znaleźć się również te dotyczące bezpośrednio pracowników[25]. Należy mieć na uwadze, że zdarzenie to dotknęło największego polskiego twórcy gier komputerowych, a więc przedsiębiorstwa, które prawdopodobnie było chronione znacznie lepiej niż przeciętna polska firma. Jest to z pewnością jeden z najgłośniejszych przypadków włamań do sieci informatycznych nie tylko w Polsce, ale i na świecie, a skala strat nim spowodowanych jest niezwykle wysoka. Sam wyciek kodów źródłowych produkcji studia, która opiera się na prawie własności intelektualnej, był realnym zagrożeniem dla przedsiębiorstwa.

Trudno jednoznacznie określić, które państwa są najczęściej celami ataków ze strony hakerów. Wydaje się jednak, że Polska nie jest w ścisłej czołówce. Ten przywilej należy do Stanów Zjednoczonych, Japonii, Bazylii, Kanady, czy Australii i Meksyku.

Innym, stosunkowo niedawnym i głośnym atakiem hakerskim, który doprowadził do poważnych konsekwencji było włamanie na giełdę kryptowalut FTX, w wyniku którego skradziono 415 milionów dolarów. Z tej kwoty udało się odzyskać jedynie 5 milionów dolarów w kryptowalutach, a straty, jakie poniosła firma, doprowadziły do jej bankructwa[26].

Ofiarami cyberprzestępców padają także bardzo znane firmy. W 2019 r. Toyota Boshoku Corporation, a więc firma produkująca części dla koncernu Toyota, straciła około 37 milionów dolarów. W tym przypadku scenariusz hakerów był stosunkowo prosty, podszyli się oni pod kontrahenta z zagranicy i wysłali wiadomość do księgowości spółki z nowym numerem konta do rozliczeń[27].

Powyższe przypadki pokazują, że nawet pojedynczy atak może być niezwykle kosztowny dla firmy. W tym miejscu warto wspomnieć o najbardziej kosztownych z nich. W 2017 r. na skutek ataku ransomware firma ExPetr straciła około 7,9–10 miliardów dolarów. W 2011 r. wyciek danych z firmy Epsilon kosztował firmę 3,1–4 miliardy dolarów, a w 2000 r. Mafiaboy na skutek ataku DDoS stracił 0,8–1 miliarda dolarów[28].

Wskazane powyżej przykłady pokazują, jak ważna dla przedsiębiorców jest ochrona systemów informatycznych. Pojedynczy udany atak przestępców może bowiem zagrozić istnieniu całej firmy.

3) Państwa

W tym podrozdziale przyjrzymy się bezpieczeństwu zarówno samej administracji państwowej, jak i wszelkich podmiotów zależnych od władz, w tym strategicznych firm, czy armii. Podmioty te odpowiadają za bezpieczeństwo społeczeństwa w wielu aspektach, nie tylko w zakresie obronności, ale także np. ruchu drogowego, kolejowego, lotniczego, energetycznego, zdrowotnego, informacyjnego etc.

Trudno jednoznacznie określić, które państwa są najczęściej celami ataków ze strony hakerów. Wydaje się jednak, że Polska nie jest w ścisłej czołówce. Ten przywilej zgodnie z danymi BlackBerry należy kolejno do Stanów Zjednoczonych (aż 65 proc. ataków), Japonii (8 proc.), Brazylii (6 proc.), Kanady (5 proc.), czy Australii i Meksyku

25 Por. https://www.wirtualnemedia.pl/artykul/cd-projekt-atak-hakerzy-wyciek-danych; https://crn.pl/aktualnosci/wykradzione-dane-cd-projektu-kraza-w-sieci; https://spidersweb.pl/2021/02/cd-projekt-nie-bylo-licytacji-wyciek-danych.html, (dostęp na dzień 08.11.2023 r.).

26 https://www.money.pl, (dostęp na dzień 08.11.2023 r.).

27 https://www.forbes.com/sites/leemathews/2019/09/06/toyota-parts-supplier-hit-by-37-million-email-scam/?sh=77fb74a75856, (dostęp na dzień 08.11.2023 r.).

28 https://www.businessleader.co.uk/what-are-the-most-expensive-cyber-attacks-of-all-time; https://www.linkedin.com/pulse/six-costliest-cyberattacks-history-shieldsupport, (dostęp na dzień 08.11.2023 r.).

(po 4 proc.)[29]. Dane te pokazują jednak ilość skutecznie odpartych ataków przez oprogramowanie pochodzące od BlackBerry. Wskazać jednak można, że **nasz kraj jest wymieniany jako dziesiąty pod względem odsetka komputerów zarażonych szkodliwym oprogramowaniem** według artykułu prezentowanego przez Cybersecurity Insiders[30].

Określając ogólny poziom cyberbezpieczeństwa Polski na tle innych krajów, możemy sięgnąć do cykliczne ukazujących się zbiorczych zestawień. Warto posłużyć się choćby rankingiem NCSI (National Cyber Security Index), w którym Polska zajmuje bardzo dobrą 11. pozycję. Co warto zaznaczyć, wszystkie miejsca od 1 do 13 zajmują państwa europejskie, a w pierwszej 30 rankingu są jedynie pojedyncze kraje z innych kontynentów. Co ciekawe, państwa posiadające bardzo wysoki poziom rozwoju cyfrowego, również prezentowanego przez NCSI, znajdują się często na znacznie dalszych pozycjach niż Polska. Dla przykładu Korea Południowa jest na 34. pozycji, USA na 46., a Japonia na 52.[31] Kraje te, zgodnie z rankingiem, posiadają ujemną relację między poziomem rozwoju a poziomem bezpieczeństwa, choć z pewnością są wymieniane w gronie gigantów informatycznych świata i stosowane w nich rozwiązania w zakresie bezpieczeństwa zarówno na szczeblu państwowym, jak i organizacji należy uznać za wiodące.

Kolejnym cennym źródłem danych o najbezpieczniejszych cyfrowo krajach są informacje firmy Kaspersky kompleksowo przedstawione przez portal Comaritech (dane z 2022 r.). Zgodnie z nimi do ścisłej czołówki państw pod tym względem należy Dania, Szwecja i Irlandia. Za najbardziej niebezpieczne uznaje się Tadżykistan, Bangladesz i Chiny. **Polska w rankingu najbardziej narażonych na cyberataki państw zajmuje bezpieczną 59. pozycję na 75 krajów**[32].

Stan cyberbezpieczeństwa państwa (kluczowych instytucji rządowych) w Polsce monitorowany jest przez CSIRT GOV. W najnowszym *Raporcie o stanie bezpieczeństwa cyberprzestrzeni RP w 2022 r.* znalazła się informacja, że **agencja zarejestrowała w ubiegłym roku łącznie 1 234 040 zgłoszeń o potencjalnym wystąpieniu incydentu teleinformatycznego**. 21 563 zdarzenia zostały zakwalifikowane jako incydenty bezpieczeństwa informatycznego. Wśród incydentów zgłaszanych przez podmioty krajowego systemu cyberbezpieczeństwa najwięcej dotyczyło operatorów infrastruktury krytycznej (1789 przypadków), urzędów (809), pozostałych podmiotów (650), organów państwowych (599), ministerstw (503), instytucji (400) i służb (200). Incydenty zgłaszane w ramach systemu ARAKIS GOV również wskazują, że zdecydowanie najwięcej ataków dotyczy infrastruktury krytycznej w Polsce (5547), następnie

29 https://www.blackberry.com/content/dam/bbcomv4/global/pdf/0408-Threat-ReportV17.pdf, (dostęp na dzień 08.11.2023 r.).
30 https://www.cybersecurity-insiders.com/list-of-countries-which-are-most-vulnerable-to-cyber-attacks, (dostęp na dzień 08.11.2023 r.).
31 https://ncsi.ega.ee/ncsi-index/?order=rank, (dostęp na dzień 08.11.2023 r.).
32 https://www.comparitech.com/blog/vpn-privacy/cybersecurity-by-country, (dostęp na dzień 08.11.2023 r.).

instytucji (2758) urzędów (2301), ministerstw (2197), pozostałych podmiotów (2189), organów państwowych (1262) i służb (350)[33].

Interesujące są również informacje dotyczące tego, skąd najczęściej pochodzą ataki cybernetyczne. Analiza przeprowadzona przez Cyber Proof wskazuje, że w 2021 r. najbardziej aktywne były Chiny (18,83 proc. ataków), Stany Zjednoczone (17 proc.), Brazylia (5,6 proc.), Indie (5,3 proc.), Niemcy (5,1 proc.), Wietnam (4,2 proc.), Tajlandia (2,5 proc.), Rosja i Indonezja (po 2,4 proc.) oraz Holandia (2,2 proc.)[34]. Dane te dotyczą całości ataków bez rozróżnienia na to kogo dotyczą i zawierają najpopularniejsze rodzaje cyberprzestępstw.

W Polsce działa kilka wyspecjalizowanych instytucji i jednostek zajmujących się cyberbezpieczeństwem na szczeblu państwa i jego instytucji. Przede wszystkim ustawa o krajowym systemie cyberbezpieczeństwa ustanowiła trzy Zespoły Reagowania na Incydenty Bezpieczeństwa Komputerowego: CSIRT NASK, wspomniany już CSIRT GOV oraz CSIRT MON.

CSIRT NASK, który prowadzony jest przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy odpowiada przede wszystkim za monitorowanie i obsługę zdarzeń naruszających bezpieczeństwo w sieci jako ogółu. Posiada kompetencje zarówno dotyczące podmiotów prywatnych, jak i publicznych. CSIRT GOV prowadzony przez Agencję Bezpieczeństwa Wewnętrznego koncentruje się z kolei na bezpieczeństwie systemów teleinformatycznych organów administracji publicznej, które są kluczowe dla ciągłości funkcjonowania państwa. CSIRT MON prowadzony przez Ministerstwo Obrony Narodowej odpowiada z kolei za bezpieczeństwo podmiotów podległych MON, infrastrukturę krytyczną, czy przedsiębiorstwa o szczególnym znaczeniu gospodarczo-obronnym[35]. W ramach poszczególnych służb działają również wyspecjalizowane jednostki, takie jak np. Centralne Biuro Zwalczania Cyberprzestępczości w Policji. O tym, jak wygląda w praktyce działanie tych instytucji i co można potencjalnie poprawić, rozmawiano między innymi podczas Forum Ekonomicznego w Karpaczu. Eksperci wskazywali, że instytucje są niedofinansowane i trudno konkurować im o prawdziwych specjalistów, którzy na rynku mogą liczyć na bardzo atrakcyjne stawki. Choć w tym zakresie następuje pewna, aczkolwiek powolna poprawa. Podkreślano, że mamy strategię cyberbezpieczeństwa i finansujemy pracę agencji, ale nie mamy środków na realizację bardziej złożonych celów. Wskazano również konieczność bardziej ścisłej współpracy w ramach UE oraz być może stworzenie Funduszu Reagowania Kryzysowego, który byłby przeznaczony na realizację zadań wymagających pilnej odpowiedzi (choć w tej kwestii głosy są podzielone). Jak podkreślają eksperci, mimo że operatorzy średnio przeznaczają 600 tysięcy euro na kwestie związane z cyberbezpieczeństwem, to żadna kwota nie będzie wystarczająca i zawsze jest coś, co można zrobić lepiej[36].

Jak wygląda w praktyce ochrona cybernetyczna Polski na tle innych państw i do czego mogą prowadzić zaniedbania w tym zakresie, pokazują liczne doniesienia medialne o spektakularnych i bardzo niebezpiecznych zdarzeniach.

Jak wygląda w praktyce ochrona cybernetyczna Polski na tle innych państw i do czego mogą prowadzić zaniedbania w tym zakresie, pokazują liczne doniesienia medialne o spektakularnych

33 CSIRT GOV, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w roku 2022.*
34 https://blog.cyberproof.com/blog/which-countries-are-most-dangerous, (dostęp na dzień 08.11.2023 r.).
35 https://www.gov.pl/web/cyfryzacja/zespol-reagowania-na-incydenty-bezpieczenstwa-komputerowego-csirt, (dostęp na dzień 08.11.2023 r.).
36 https://cyberdefence24.pl/cyberbezpieczenstwo/ile-kosztuje-nas-cyberbezpieczenstwo, (dostęp na dzień 08.11.2023 r.).

i bardzo niebezpiecznych zdarzeniach. Z pewnością jednym z nich jest wyciek ogromnej bazy danych o sprzęcie i brakach w polskiej armii, do którego doszło 9 stycznia 2022 r. Lista zawierała ponad 1,7 miliona wpisów zwierających strategiczne informacje wojskowe zarówno o podstawowej broni i amunicji, aż po informacje dotyczące samolotów F-16. Na liście znajdowały się zapotrzebowania na mundury czy bieliznę, jak i specjalistyczną broń i wyposażenie wojska. Trudno przecenić wagę problemu i niebezpieczeństwo dla obronności Polski tego zdarzenia w kontekście choćby wojny toczącej się za naszą wschodnią granicą[37].

O niezwykle niebezpiecznej luce w bezpieczeństwie kolejowym informuje między innymi Najwyższa Izba Kontroli. Od lat cyklicznie dochodzi do niebezpiecznych naruszeń w przestarzałym systemie awaryjnego zatrzymywania pociągów. Okazuje się, że jest on oparty na sygnale radiowym, który w sposób bardzo prosty można nadać dostępnymi powszechnie urządzeniami, powodując paraliż ruchu kolejowego. Do tego rodzaju zdarzeń doszło również w tym roku. 27 sierpnia zatrzymano pociągi w pobliżu stacji Łapy, a 29 sierpnia użyto sygnału na stacji Łódź Kaliska i w Gomunicach[38]. NIK informuje, że PKP PLK SA nie zainstalowała nowoczesnego systemu GSM-R, czyli łączności cyfrowej dla kolei na żadnym odcinku linii, w których system powinien być wdrożony w ramach projektu „Budowa infrastruktury systemu ERTMS GSM-R na liniach kolejowych PKP PLK S A w ramach NPW ERTMS", a całość linii objętej systemem wg stanu na 30 czerwca 2022 r. to zaledwie 884,2 km. Drugi z nowoczesnych systemów sterowania ruchem pociągów – ETCS w okresie objętym kontrolą został zainstalowany jedynie na odcinku 500 km, czyli jednej czwartej wielkości planowanej w Krajowym Programie Kolejowym do osiągnięcia w 2023 r.[39] Jest to z pewnością bardzo niebezpieczna luka w systemach bezpieczeństwa polskiej kolei, która może prowadzić do realnych zagrożeń dla pasażerów. Zważywszy na przywołane wcześniej dane CSIRT GOV wskazujące, że to infrastruktura krytyczna jest najczęściej celem cyberataków, to z pewnością przestarzały system bezpieczeństwa kolejowego jest bardzo wrażliwy na potencjalne ataki.

W podrozdziale dotyczącym bezpieczeństwa organizacji opisane zostały przykłady ataków BEC np. na Toyotę. Wskazać należy, że podobne

37 https://www.newsweek.pl/polska/spoleczenstwo/wyciek-danych-z-wojska-z-armii-wyciekla-baza-danych-o-sprzecie/x6vtz4t; https://www.rp.pl/wojsko/art19288261-strategiczne-dane-wojska-polskiego-wyciekly-do-sieci-mon-sprawa-jest-analizowana, (dostęp na dzień 8.11.2023 r.).

38 https://www.rmf24.pl/regiony/lodz/news-pociagi-znow-sie-zatrzymaly-uzyto-sygnalu-radio-stop,nId,6992445#crp_state=1; https://www.pap.pl/aktualnosci/zatrzymanie-pociagow-po-sygnalach-radio-stop-obroncy-chca-podejrzani-wyszli-z-aresztu, (dostęp na dzień 08.11.2023 r.).

39 https://www.nik.gov.pl/aktualnosci/kolej-radio-stop.html, (dostęp na dzień 08.11.2023 r.).

zdarzenie dotknęło spółkę Cenzin związaną z Polską Grupą Zbrojeniową. Cyberprzestępcy również w tym przypadku wysłali do firmy maila z informacją o zmianie konta do rozliczeń, podszywając się pod kontrahenta. Wiadomość ta nie została odpowiednio zweryfikowana, a spółka zastosowała się do wskazań przestępców, tracąc 4 miliony złotych[40].

Również na szczeblu rządowym czasem dochodzi do wycieku poufnych danych. Najczęściej przyczyną jest błąd ludzki i niezachowanie zasad bezpieczeństwa. Jednym z głośniejszych przypadków tego rodzaju zdarzeń w ostatnich latach był wyciek maili z Kancelarii Prezesa Rady Ministrów. Media informowały, że **wśród licznych informacji, które miały ujrzeć światło dzienne na skutek włamania na skrzynkę pocztową Michała Dworczyka, miały znaleźć się również informacje tajnne.** Znaczącym problemem w tej sprawie jest to, że do włamania miało dojść z powodu wykorzystywania prywatnych kont pocztowych. **Sprawa ta do dziś nie została wyjaśniona, ale jeśli doniesienia medialne okażą się prawdziwe, to z pewnością jest to jeden z najpoważniejszych incydentów w zakresie cyberbezpieczeństwa w ostatnich latach**[41].

Rola, jaką Polska odgrywa jako sojusznik Ukrainy w wojnie z Rosją, również prowadzi do wzrostu zainteresowania cyberprzestępców naszym krajem. Jak donoszą media w ostatnich dniach prokremlowskie grupy „Cyber Army of Russia" oraz „NoName057(16)" dokonały licznych ataków DDoS na serwery kluczowych instytucji i firm między innymi na strony internetowe Poczty Polskiej czy Portu Lotniczego Warszawa–Modlin. Atakowane miały być również strony rządowe, Izby Skarbowej, straży granicznej oraz systemy kolejowe. Jak wskazują eksperci takich ataków w ostatnim czasie jest coraz więcej[42].

Mimo wszystko Polska wciąż nie jest krajem, który jest najczęściej atakowany przez cyberprzestępców. Najbardziej atrakcyjnym dla nich celem są z pewnością największe mocarstwa na świecie jak np. USA, a także państwa, które są w ścisłym centrum konfliktów, jak Izrael, czy Tajwan, które opiszemy oddzielnie.

Jak informuje portal Politico w ostatnich latach doszło do serii wysokospecjalistycznych cyberataków na USA ze strony Rosji, Chin i organizacji przestępczych, co było przyczyną zmiany podejścia Departamentu Obrony do walki cybernetycznej[43]. Przykładem takich zdarzeń może być niedawny atak chińskich hakerów, który doprowadził do przejęcia maili Sekretarza Handlu Gina Raimondo oraz innych osób pracujących w Departamencie Stanu. W tym przypadku przestępcy wykorzystali lukę w usługach poczty Microsoftu[44]. Również infrastruktura krytyczna w USA jest celem cyberprzestępców. Przykładem jest prawdopodobnie największy w historii udany atak na infrastrukturę olejową Colonial Pipeline, do którego doszło w 2021 r. Rurociąg, który zaopatruje blisko połowę Wschodniego Wybrzeża w paliwa, został w wyniku ataku całkowicie wyłączony, powodując istotne utrudnienia. Przestępcy wykorzystali w tym celu działania typu ransomware[45]. Pokazane przykłady wskazują, że również giganci w zakresie technologii informatycznych jak USA mają problemy z zapewnieniem bezpieczeństwa swoich systemów. Stały rozwój zagrożeń skłonił

40 https://pieniadze.rp.pl/finanse-firmy/art36817681-najkosztowniejsze-cyberataki-dla-firm-straty-ida-w-miliony, (dostęp na dzień 08.11.2023 r.).

41 https://tvn24.pl/polska/afera-mailowa-prokuratura-wszczela-sledztwo-w-sprawie-maili-michala-dworczyka-doszlo-o-ujawnienia-tajemnic-panstwowych-6784987; https://www.rp.pl/polityka/art38044011-afera-mailowa-tajne-informacje-w-wiadomosciach-ze-skrzynki-dworczyka-jest-sledztwo, (dostęp na dzień 08.11.2023 r.).

42 https://cyfrowa.rp.pl/it/art39364831-rosyjski-atak-na-poczte-i-modlin-za-ukraine, (dostęp na dzień 08.11.2023 r.).

43 https://www.politico.com/news/2023/09/12/pentagon-cyber-command-private-companies-00115206, (dostęp na dzień 08.11.2023 r.).

44 https://www.politico.com/news/2023/07/12/chinese-hackers-government-emails-microsoft-breach-00105879, (dostęp na dzień 08.11.2023 r.).

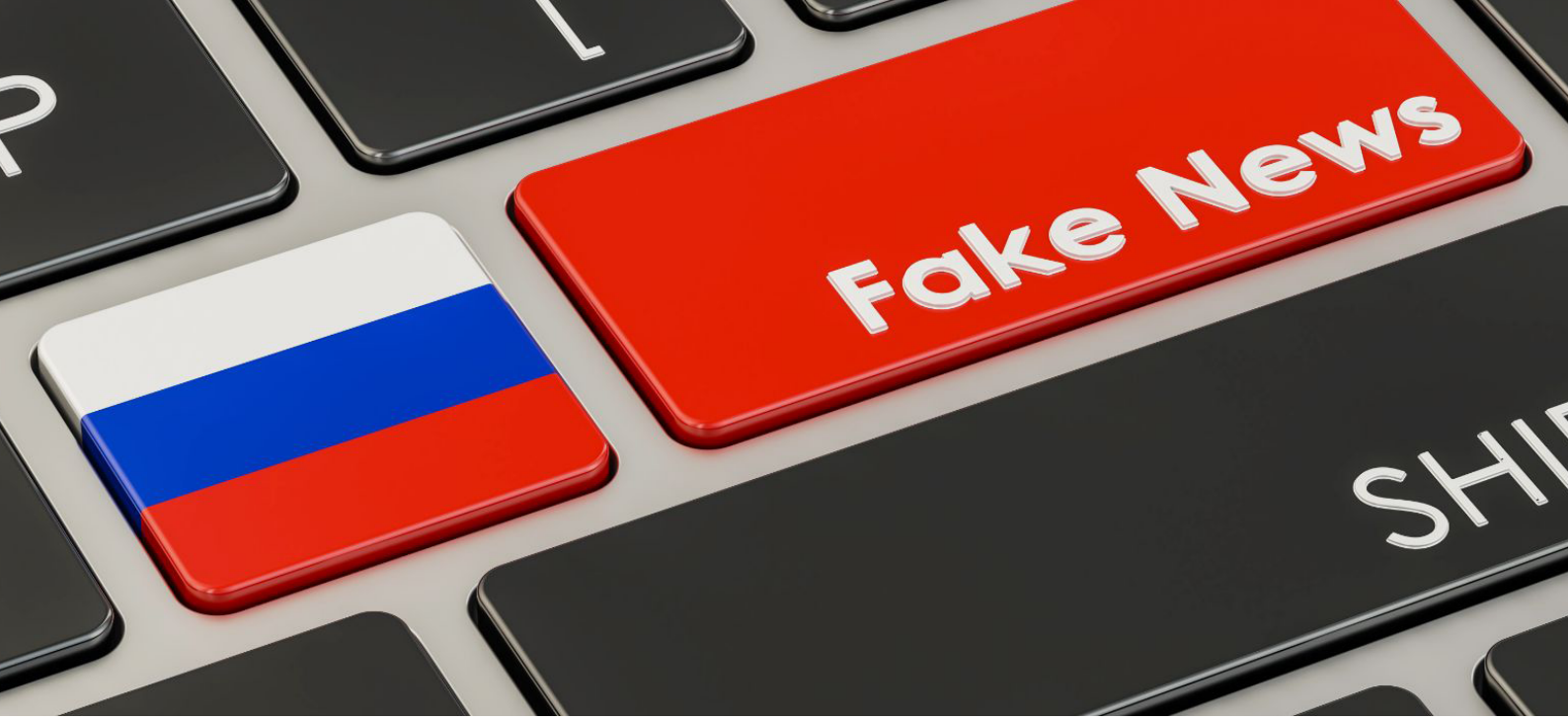
45 https://www.politico.com/news/2021/05/08/colonial-pipeline-cyber-attack-485984, (dostęp na dzień 08.11.2023 r.).

amerykański Departament Obrony do przyjęcia nowej strategii cyberbezpieczeństwa w 2023 r.

Warto wspomnieć także o poważnym w skutkach ataku hakerskim, jaki dotknął Grecję w tym roku. Został on skierowany przeciwko systemom ministerstwa edukacji i doprowadził do zakłócenia egzaminów w szkołach średnich. Do jego przeprowadzenia wykorzystano urządzenia ze 114 krajów. Atak miał charakter DDoS, czyli rozproszoną odmowę dostępu do usługi i miał na celu zajęcie wszystkich dostępnych zasobów celu w taki sposób, aby uniemożliwić funkcjonowanie usługi[46].

Przytoczone przykłady z całą pewnością pokazują, jak niebezpieczne dla funkcjonowania całego państwa mogą być ataki cyberprzestępców. Należy szczególną uwagę poświęcić tej kwestii w przyszłości również z uwagi na stałą informatyzację systemów bezpieczeństwa wojskowego. Nowoczesne technologie siłą rzeczy są bowiem wykorzystywane powszechnie w armii, a przejęcie kontroli nad nimi przez cyberprzestępców może stanowić niewyobrażalne ryzyko. Podobnie prezentuje się również sytuacja w zakresie systemów finansowych, sieci naukowych i tworów własności intelektualnej o strategicznym znaczeniu, czy całej infrastrukturze państwowej.

[46] https://cyberdefence24.pl/cyberbezpieczenstwo/najpowazniejszy-cyberatak-w-historii-grecji-dotknal-resort-edukacji-i-zaklocil-egzaminy, (dostęp na dzień 08.11.2023 r.).



4. Wzrost znaczenia cyberbezpieczeństwa w dobie niepokojów geopolitycznych

- **Izrael będąc w stałym napięciu spowodowanym trwającym od lat sporem z Palestyną, w 2017 roku stworzył agencję Israel National Cyber Directorate. Jest to instytucja odgrywająca kluczową rolę dla cyberbezpieczeństwa Izraela, na której mogłaby wzorować się również Polska przy tworzeniu podobnych struktur.**
- **Innym sposobem „walki" na cyfrowym polu bitwy w ostatnich latach jest propaganda i dezinformacja. Jest to niezwykle skuteczne narzędzie w rękach władz i podmiotów sprzyjających Rosji w agresji na Ukrainę.**
- **Po tym jak władze Estonii zdecydowały się na przeniesienie w 2007 r. pomnika Brązowego Żołnierza z Tallinna, państwo to stało się celem zmasowanych ataków cyberprzestępców. O ataki podejrzewana była Federacja Rosyjska, a walka o wpływy rosyjskie w Estonii trwa do dziś.**
- **Cybernetyczna wojna trwa także między Chinami a Tajwanem. Doniesienia mówią nawet o 5 milionach ataków cybernetycznych różnego rodzaju skierowanych przeciwko Tajwanowi każdego dnia.**
- **Tak jak w Estonii, tak również na Tajwanie dezinformacja stała się narzędziem walki, jednak w tym przypadku znacznie bardziej agresywnej i bezpośredniej.**

W niniejszym rozdziale przedstawimy informacje dotyczące rosnącego znaczenia wojny cybernetycznej w dobie pojawiających się niepokojów geopolitycznych między innymi w Izraelu, Estonii, czy na Tajwanie. Należy jednak na wstępie podkreślić, że dane dotyczące strategicznego bezpieczeństwa są ściśle chronione przez każde państwo (całkowicie słusznie), a informacje przedstawione poniżej pochodzą z mediów oraz licznych wypowiedzi ekspertów. Ponadto wiele organizacji przypisuje sobie „zasługi" na polu wojny cybernetycznej jedynie dla poklasku i trudno ze 100-procentową pewnością wskazać winnych poszczególnych ataków. Ponadto wiele grup hakerskich, choć powołuje się na względy ideologiczne, w rzeczywistości współpracuje blisko z władzami poszczególnych państw.

1) „Haktywiści" i wojna

W ostatnich tygodniach na nowo rozgorzał konflikt izraelsko-palestyński, który już w pierwszych tygodniach obfitował w tragiczne wydarzenia skutkujące śmiercią nie tylko wojskowych, ale również bardzo wielu cywili. Zdarzenia te pokazały, jak istotną rolę w dzisiejszych czasach odgrywają działania zarówno ofensywne, jak i defensywne w zakresie cyberbezpieczeństwa.

Izrael będąc niewielkim państwem, które posiada ograniczone zasoby w porównaniu do największych i najbogatszych krajów, a jednocześnie będąc w stałym napięciu spowodowanym trwającym od lat sporem z Palestyną, zdawał sobie sprawę z konieczności zabezpieczenia się na polu cyberbezpieczeństwa. W związku z tym podjęto decyzję, by w 2017 roku stworzyć agencję Israel National Cyber Directorate. Jest to unikatowa i strategiczna instytucja mająca na celu wymianę informacji z wszelkimi agencjami rządowymi, wywiadem, kontrwywiadem, instytucjami prywatnymi i międzynarodowymi. INCD buduje sojusze, również międzynarodowe, i dba o odpowiednie relacje. Agencja ma wpływ na instytucje państwowe i dba o kwestie odpowiedniego zabezpieczenia kraju pod względem ataków cybernetycznych. Oczywiście szczegóły poszczególnych działań organizacji nie są znane, natomiast będąc centralnym organem i swego rodzaju hubem informacyjnym i decyzyjnym w wielu aspektach jest ona w stanie działać efektywnie i jest chwalona przez ekspertów[47]. Jest to z pewnością instytucja odgrywająca kluczową rolę dla cyberbezpieczeństwa Izraela, na której mogłaby wzorować się również Polska przy tworzeniu podobnych struktur. Wskazać jednak należy, że paradoksalnie duże skupienie się Izraela na cyberbezpieczeństwie mogło doprowadzić do przeoczenia zagrożenia ze strony Hamasu w kontekście ataku, którą ta organizacja przeprowadziła 7 października 2023 r. Organizacja stworzyła rozbudowaną sieć kryjówek, w tym tuneli podziemnych, które umożliwiają bardzo efektywne ukrywanie się i prowadzenie działań. Działając „staroświecko", byli prawdopodobnie w stanie w dużej mierze pozostawać niezauważeni przez odpowiednie służby Izraela, choć oczywiście szczegóły działań tych służb nie są dostępne publicznie[48].

O ile Izrael chwalony jest za bardzo dobre i skoordynowane działania na rzecz bezpieczeństwa cybernetycznego państwa, to mimo to nie był w stanie uchronić się przed licznymi cyberatakami. Media donoszą o licznych atakach DDoS oraz wykorzystujących inżynierię społeczną na systemy kluczowej infrastruktury dla tego państwa. Największą panikę wywołały jednak działania dezinformacyjne, które przypisuje sobie grupa haktywistów „AnonGhost". Włamali się oni do popularnej aplikacji do ostrzegania przed niebezpieczeństwem w Izraelu i wysłali między innymi alarmy o zbliżającym się ataku nuklearnym[49]. Tego rodzaju działania grup „haktywistów", czyli zorganizowanych grup hakerskich, które deklarują, że działają z pobudek ideologicznych i angażują się w liczne ataki na całym świece, stały się ostatnio niezwykle popularne. Kolejnym bardzo poważnym w skutkach atakiem na Izrael w ostatnim czasie były zorganizowane działania DDoS na licznych serwerach izraelskich np. niezwykle popularnego dziennika „The Jerusalem Post". Serwis ten udało się wyłączyć na cały dzień. Do tych działań przyznaje się grupa Anonymous Sudan. W całym kraju ofiarami podobnych incydentów padło również wiele innych popularnych stron internetowych. Celem takich akcji jest odcięcie społeczeństwa od informacji i szerzenie paniki[50].

Izrael chwalony jest za bardzo dobre i skoordynowane działania na rzecz bezpieczeństwa cybernetycznego państwa, to mimo to nie był w stanie uchronić się przed licznymi cyberatakami.

Serwery rządowe Izraela również zostały zaatakowane przez grupę KillNet powiązaną z Rosją. Hakerzy twierdzą, że w 2022 r. Izrael zdradził Rosję,

47 M. Miron, King's College London w wywiadzie dla DW News, https://www.youtube.com/watch?v=bXlQvRoYaiA, (dostęp na dzień 08.11.2023 r.).

48 https://fakty.tvn24.pl/fakty-o-swiecie/hamas-stworzyl-podziemna-siec-tuneli-to-idealne-miejsca-na-zasadzki-czy-umieszczanie-min-7421794, (dostęp na dzień 08.11.2023 r.).

49 https://cybernews.com/cyber-war/israel-redalert-breached-anonghost-hamas, (dostęp na dzień 08.11.2023 r.).

50 https://www.politico.eu/article/israel-hamas-war-hackers-cyberattacks, (dostęp na dzień 08.11.2023 r.).

wspierając Ukrainę. W związku z czym haktywiści postanowili aktywnie wspierać w toczącym się konflikcie Palestynę i zaatakowali bezpośrednio systemy informatyczne władz Izraela. Dokonano także licznych ataków na firmy energetyczne, obronne, telecomy, czy instytucje finansowe. Doniesienia medialne wskazują na grupę Strom-1133[51]. Ofiarami ataków padła także druga największa elektrownia izraelska „DORAD". Grupa „Cyber Avengers" opublikowała liczne dokumenty wewnętrzne oraz włamała się do systemu monitoringu, choć prawdopodobnie obecnie nie jest w stanie bezpośrednio zakłócić jej funkcjonowania[52].

Należy mieć na względzie, że działania „haktywistów" w historii były oceniane bardzo różnie, a część z nich ma wielu zwolenników na całym świecie. Zapewne wiele z tych grup działa z pobudek czysto ideologicznych, ale przyjąć należy, że wiele posiada przynajmniej pewne powiązania polityczne i wspiera określone działania rządów konkretnych państw.

2) Dezinformacja narzędziem walki

Innym sposobem „walki" na cyfrowym polu bitwy w ostatnich latach jest propaganda i dezinformacja. Jest to niezwykle skuteczne narzędzie w rękach władz i podmiotów sprzyjających Rosji w agresji na Ukrainę. Zarówno przed napaścią na ten kraj, jak i od początku walk, w sieci krążą tysiące nieprawdziwych informacji mających na celu szerzenie prokremlowskiej wizji świata.

Zacznijmy jednak od wydarzeń, które są najsłynniejszym i najpoważniejszym atakiem przeprowadzonym przeciwko konkretnemu państwu. Po tym, jak władze Estonii zdecydowały się na przeniesienie w 2007 r. pomnika Brązowego Żołnierza z Tallinna, państwo to stało się celem zmasowanych ataków cyberprzestępców. W ich trakcie ucierpiały strony licznych organizacji w tym parlamentu, banków, ministerstw, gazet, czy mediów. Większość z incydentów miała charakter Denial of Service, które zakłóciły na pewien czas funkcjonowanie państwa. O ataki podejrzewana była Federacja Rosyjska[53], a walka o wpływy rosyjskie w Estonii trwa do dziś. Kraj ten jest bowiem jedną z byłych republik bałtyckich wchodzących w skład Związku Radzieckiego i wciąż żyje w nim wiele osób, które porozumiewają się wyłącznie językiem rosyjskim. To właśnie ta grupa osób jest „łatwym celem" dla propagandzistów. Rosja bezpośrednio graniczy z Estonią, a dostęp do mediów prokremlowskich

51 https://securityaffairs.com/152153/hacking/gaza-linked-hackers-argeting-israel.html, (dostęp na dzień 08.11.2023 r.).
52 https://www.youtube.com/watch?v=6zYloNKD-08, (dostęp na dzień 08.11.2023 r.).
53 https://en.wikipedia.org/wiki/2007_cyberattacks_on_Estonia, (dostęp na dzień 08.11.2023 r.).

jest całkowicie swobodny – nie ma bowiem możliwości zablokowania sygnału telewizyjnego z sąsiedniego kraju. I to właśnie ta telewizja jest często jedynym źródłem informacji dla rosyjskojęzycznych mieszkańców Estonii. Poza telewizją regularnie wykorzystywane są media społecznościowe, komunikatory i wszelkie rosyjskojęzyczne portale internetowe. W Internecie działają liczne „farmy trolli", czyli zorganizowane grupy opłacane przez prorosyjskie środowiska, których jedynym celem jest publikowanie prorosyjskich treści i komentarzy. Dotyczy to nie tylko Estonii, ale również Polski i wielu innych państw na świecie. W takich warunkach bardzo trudno jest uniknąć budowania fałszywego obrazu rzeczywistości u znacznej części estońskiego społeczeństwa, a to stało się szczególnie niebezpieczne od czasu agresji rosyjskiej na Ukrainę.

Jedną z pierwszych odpowiedzi estońskich władz na to zagrożenie było wprowadzenie już osiem lat temu kanału telewizyjnego w języku rosyjskim, po to, aby stanowił on alternatywę dla rosyjskich mediów. Estonia wykorzystuje jednak znacznie bardziej interesujące metody dla ochrony przed propagandą. Tworzone są między innymi różnego rodzaju kursy, na których rosyjskojęzyczni obywatele mogą nauczyć się np. wypiekać pizzę, a jednocześnie uczyć języka estońskiego[54]. Takie niekonwencjonalne metody sprzyjają większej integracji społeczeństwa, a to może odciągnąć ich od korzystania z mediów prokremlowskich mających na celu wzbudzanie niepokoju i niezadowolenia społecznego oraz budowania fałszywego obrazu napaści Rosji na Ukrainę.

3) Życie „pod ostrzałem" cyberataków

Z pewnością bardzo jaskrawym przypadkiem funkcjonowania będąc pod stałym ostrzałem cybernetycznych ataków, jest Tajwan. Ta niewielka demokratyczna wyspa, która uważana jest przez Chiny za część ich terytorium, od lat żyje w ryzyku wystąpienia konfliktu zbrojnego. Choć ryzyko jest realne, to Chiny mimo wszystko nie zdecydowały się na podjęcie bezpośrednich kroków, jednak podejmują rozliczne działania mające na celu osłabić, czy podporządkować Tajwan ich rządom. Doskonale w tym celu sprawdzają się narzędzia cybernetyczne.

Eksperci i media wskazują wprost, że między Chinami a Tajwanem trwa cybernetyczna wojna. Doniesienia mówią nawet o 5 milionach ataków cybernetycznych różnego rodzaju skierowanych przeciwko Tajwanowi każdego dnia. Większość z nich pochodzi z terytorium Chin. Każdego dnia zdarzają się incydenty kierowane przeciwko publicznemu transportowi, sieciom energetycznym, czy szpitalom. Tajwan jest świadom zagrożeń i rozwija zaawansowane metody ich zwalczania. Jednym z tego rodzaju rozwiązań są specjalne agencje wykrywające i zwalczające zagrożenia, jak „Team T5". Grupa specjalistów z tej instytucji była w stanie zidentyfikować wielu chińskich hakerów, których dane i wizerunki zostały ujawnione i którzy są obecnie poszukiwani nie tylko przez Tajwan, ale np. przez amerykańskie FBI[55].

Tak jak w Estonii, tak również na Tajwanie dezinformacja stała się narzędziem walki, jednak w tym przypadku znacznie bardziej agresywnej i bezpośredniej. Osoby zaangażowane w ten proces wykorzystują np. niezwykle popularny komunikator „Line", który jest źródłem informacji dla wielu Tajwańczyków. Za jego pomocą, a także wielu innych mediów, Chiny szerzą dezinformację, propagandę i niepokój wśród społeczeństwa. Skala tego zjawiska jest ogromna.

Największe obawy Tajwanu dotyczą tego, że w razie otwartego konfliktu zbrojnego, przy tej skali cybernetycznych ataków ze strony Chin, będą one w stanie wyłączyć całą krytyczną infrastrukturę, znacząco ograniczając możliwości obrony[56].

54 https://www.youtube.com/watch?v=z98sfwipeRA, (dostęp na dzień 08.11.2023 r.).
55 https://www.youtube.com/watch?v=CdYK0AWmLJg, (dostęp na dzień 08.11.2023 r.).
56 https://www.youtube.com/watch?v=Agc3vy-JD4c, (dostęp na dzień 08.11.2023 r.).

5. Poprawa cyberbezpieczeństwa Polski i wzorce z innych krajów – rekomendacje

- **Polska obecnie nie należy do najbardziej zagrożonych państw świata i radzi sobie stosunkowo dobrze z zapewnieniem bezpieczeństwa cybernetycznego. Nie oznacza to jednak, że możemy czuć się całkowicie bezpieczni.**
- **Niezrozumiałe są wycieki danych z polskich instytucji, jak choćby niezwykle ważne dane dotyczące polskiego uzbrojenia, czy tajne informacje wypływające od czołowych polityków naszego kraju. Innym problemem Polski w zakresie cyberbezpieczeństwa jest zgłaszany przez przedsiębiorców brak środków na inwestycje w tym zakresie.**
- **USA posiada odrębną i na bieżąco aktualizowaną strategię cyberbezpieczeństwa przeznaczoną wyłącznie celom obronności.**
- **Przyczyny niskiego poziomu inwestycji mają wiele wymiarów, jednak jednym z najważniejszych jest niestabilne prawo i niejasny system podatkowy.**

Przedstawione w niniejszym dokumencie dane pochodzące z raportów licznych organizacji, jak i poszczególne przykłady rzeczywistych zagrożeń wskazują wprost, że Polska obecnie nie należy do najbardziej zagrożonych państw świata i radzi sobie stosunkowo dobrze z zapewnieniem bezpieczeństwa cybernetycznego. Nie oznacza to jednak, że możemy czuć się całkowicie bezpieczni, zwłaszcza w czasach licznych niepokojów geopolitycznych i coraz częstszego wykorzystywania cyberataków nie tylko w celu wyłudzenia pieniędzy od osób fizycznych i organizacji, ale również na potrzeby szpiegostwa technologicznego, czy nawet działań destabilizujących, hybrydowych, czy wręcz terrorystycznych.

W pierwszej kolejności warto wskazać mocne strony naszego kraju. Wskazywaliśmy już badania mówiące o tym, że **polskie banki są uważane za jedne z najbezpieczniejszych w regionie**. Posiadamy bardzo dobrze rozwinięte usługi finansowe, zarówno klasyczne systemy bankowe, jak i wszelkiego rodzaju fintechy. Dla przykładu dane wskazują, że w 2022 r. w Polsce liczba transakcji bezgotówkowych wzrosła aż o 28 proc., a liczba takich transakcji przekroczyła 461 milionów. Obrót bezgotówkowych transakcji wyniósł natomiast 30,1 miliarda złotych i był wyższy o 40 proc. niż w 2021 r.[57] PolCard ponadto wskazuje, że aż 40 proc. osób mając możliwość płatności kartą,

[57] https://forsal.pl/finanse/artykuly/8654557,liczba-transakcji-bezgotowkowych-w-polsce-2022.html, (dostęp na dzień 08.11.2023 r.).

telefonem czy zegarkiem, zawsze wybiera taką możliwość, a 30 proc. robi to przynajmniej raz w tygodniu[58]. Wszystko to przekłada się na zaufanie do instytucji finansowych ze strony konsumentów. Oczywiście wysoka popularność tego typu usług jest pokusą dla przestępców, ale wskazać należy, że są oni zmuszeni do wykorzystywania przede wszystkim socjotechniki, aby wyłudzić od użytkowników usług finansowych dane niezbędne do dokonania oszustwa. Ogół przedstawionych w niniejszym dokumencie informacji wskazuje, że bezpieczeństwo usług finansowych jest w naszym kraju na dobrym poziomie. Z całą pewnością jednak konieczne jest inwestowanie w edukację społeczeństwa w zakresie cyberzagrożeń i tego, jak działają przestępcy usiłujący wykraść nasze dane osobowe.

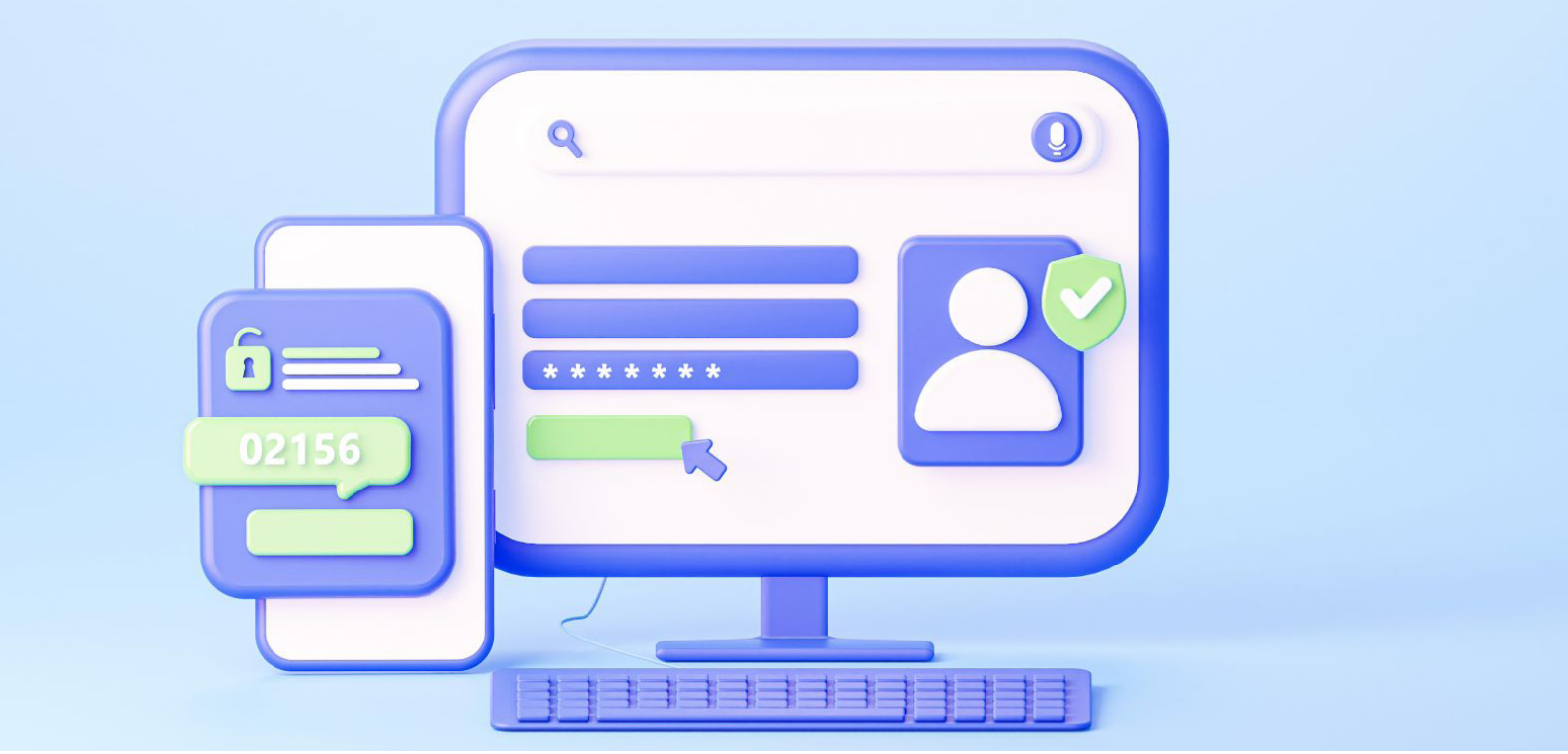
Podkreślić należy również, że banki wymieniane jako liderzy cyberbezpieczeństwa takie, jak Citibank bądź Bank of America oferują bardzo dobre zabezpieczenia przed włamaniem, które jednak są również powszechnie oferowane przez polskie banki i instytucje finansowe. Rozwiązania takie jak weryfikacja dwuetapowa, blokowanie kart debetowych, czy jednorazowe wirtualne karty do płatności online są powszechnymi rozwiązaniami również w Polsce, choć nie każda instytucja oferuje wszystkie te rozwiązania[59]. Polskie banki są także zobligowane w określonych okolicznościach do ponoszenia odpowiedzialności finansowej w razie naruszenia zabezpieczeń w ich systemach, w wyniku których doszło do utraty przez klienta środków. Na tym tle powstaje jednak sporo kontrowersji i reklamacje z tego tytułu dokonywane przez klientów często spotykają się z odmową ich uwzględnienia z uwagi na przyczynienie się klienta do utraty danych dostępowych do konta. Tego rodzaju spory często muszą być rozstrzygane przez sądy, a o ich przykładach informują media[60].

Kapitał ludzki jest jednym z najważniejszych czynników przyciągających do naszego kraju gigantów świata technologii, jak Google, czy Microsoft, które posiadają tu swoje oddziały.

Kolejną silną stroną Polski w kontekście cyberbezpieczeństwa są również rodzime zasoby kadrowe. Polscy informatycy są niezwykle cenieni na całym świecie i doceniani w licznych rankingach. Za przykład może posłużyć ranking Hackerrank, w którym polscy programiści od lat zajmują bardzo wysoką pozycję, a w ostatnim zestawieniu zajęli trzecią lokatę na świecie[61]. To właśnie kapitał ludzki jest jednym z najważniejszych czynników przyciągających do naszego kraju gigantów świata technologii, jak Google, czy Microsoft, które posiadają tu swoje oddziały. Ci utalentowani specjaliści, których posiada nasz kraj, często stoją na straży bezpieczeństwa polskich firm, banków, czy instytucji państwowych.

Gdzie Polska posiada największe braki? Wydaje się, że upatrywać ich należy w instytucjach państwowych, urzędach, czy podmiotach odpowiadających za infrastrukturę krytyczną. Wymienione w niniejszym dokumencie przykłady spektakularnych naruszeń cyberbezpieczeństwa w tym zakresie wprost pokazują, z jakimi problemami się zmagamy. **Z całą pewnością pilnej modernizacji wymaga wspomniany już system kontroli ruchu pociągów, który jest bardzo klarownym przykładem niebezpieczeństwa płynącego z wykorzystania technologii radiowej sprzed kilku dekad. Jest to o tyle niezrozumiałe, że posiadamy w tym zakresie bardzo dobre i gotowe do wdrożenia wzorce, jak system ERTMS GSM-R, który jest standardem wdrażanym w Unii Europejskiej. Biorąc pod uwagę integrację**

58 https://direct.money.pl/artykuly/porady/70-proc-polakow-przynajmniej-raz-w-tygodniu-placi-bezgotowkowo-terminal-to-juz-obowiazek,-a-nie-wybor-firm, (dostęp na dzień 08.11.2023 r.).
59 https://www.mybanktracker.com/news/most-secure-big-banks-offer-extra-account-protection, (dostęp na dzień 08.11.2023 r.).
60 https://www.prawo.pl/biznes/haker-wyprowadzil-pieniadze-z-rachunku-bank-placi,522407.html, (dostęp na dzień 08.11.2023 r.).
61 https://distantjob.com/blog/countries-to-find-best-programmers, (dostęp na dzień 08.11.2023 r.).



infrastruktury w ramach UE, Polska z pewnością powinna wzorować się na istniejących rozwiązaniach i to nie tylko w zakresie ruchu kolejowego.

Całkowicie niezrozumiałe są również wycieki danych z polskich instytucji, jak choćby niezwykle ważne dane dotyczące polskiego uzbrojenia, czy tajne informacje wypływające od czołowych polityków naszego kraju. W tym zakresie ponownie wskazać należy, że najczęstszą przyczyną tego rodzaju zdarzeń bywa błąd ludzki i niestety świadomość cyberzagrożeń okazuje się niewystarczająca często nawet na najwyższych szczeblach politycznych i wojskowych. Polska podobnie jak inne kraje posiada Strategię Cyberbezpieczeństwa[62], niemniej jednak dokument ten zawiera bardzo ogólnikowe założenia dotyczące np. wymiany informacji, monitoringu zdarzeń, czy zmian prawnych wynikających głównie z założeń dostosowania do prawa UE. Choć w dokumencie mowa jest o „działaniach odnoszących się do programów edukacyjnych, informacyjnych i szkoleniowych dotyczących cyberbezpieczeństwa", to wydaje się, że praktyczne budowanie wiedzy w tym zakresie zarówno w strukturach państwowych, jak i wśród obywateli jest stosunkowo niewielkie. **Wskazać należy również, że np. USA posiada odrębną i na bieżąco aktualizowaną strategię cyberbezpieczeństwa przeznaczoną wyłącznie celom obronności[63]. Strategia jest oczywiście tajna, a opinii publicznej przedstawione są jedynie ogólne zagrożenia i założenia, jak im przeciwdziałać. Wydaje się, że w dobie narastających konfliktów geopolitycznych, toczącej się wojny na Ukrainie oraz napięć na Bliskim Wschodzie, tego rodzaju rozwiązanie nakierowane bezpośrednio na obronność byłoby w Polsce pożądane.**

Z całą pewnością należy również zwrócić się w kierunku wzorców już wypracowanych w krajach, które dziś muszą mierzyć się z poważnymi zagrożeniami. **Na szczeblu państwowym warto byłoby rozważyć wprowadzenie agencji podobnej do Israel National Cyber Directorate, która byłaby w stanie gromadzić dane o bezpieczeństwie cybernetycznym, monitorować zagrożenia i wymieniać informacje na szczeblu centralnym, a jednocześnie posiadałaby realne narzędzia do kreowania polityki cyberbezpieczeństwa państwa *ad hoc*.** Pożądane byłoby również tworzenie jednostek podobnych do tajwańskiego „Team T5", które w sposób zorganizowany stałyby w pierwszym szeregu cybernetycznej wojny, walcząc z zagrożeniami. Efektywne prowadzenie polityki cyberbezpieczeństwa powinno odbywać się z uwzględnieniem odpo-

62 *Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024.*
63 U.S. Department of Defense, *Summary 2023 Cyber Strategy of The Department of Defense.*

wiednich środków w budżecie, gdyż jak pokazuje praktyka, bezpieczeństwo cybernetyczne nie jest mniej ważne niż wojskowe, a często jest z nim bardzo silnie powiązane.

Kolejnym istotnym problemem Polski w zakresie cyberbezpieczeństwa jest zgłaszany przez przedsiębiorców brak środków na inwestycje w tym zakresie. Można w tym miejscu posłużyć się choćby badaniem Związku Przedsiębiorców i Pracodawców „Busometr ZPP", czyli Indeksem nastrojów Gospodarczych. Jak wskazują ankietowane przedsiębiorstwa w badaniu nastrojów na I półrocze 2023 r. wskaźnik dotyczący inwestycji wyniósł 24,1 (wskaźnik liczony jest od 0 do 100, przy czym wynik powyżej 50 oznacza dobre nastroje, a poniżej złe). Jest to najgorszy rezultat w dwunastoletniej historii badania[64]. Trudno zatem dziwić się firmom ankietowanym w badaniu ESET (przywołanym uprzednio w dokumencie), że obawiają się one, że nie będą w stanie przeznaczyć na cele cyberbezpieczeństwa środków pozwalających im nadążyć za zmieniającymi się na rynku warunkami. Ostatnie lata w polskiej gospodarce odcisnęły silne piętno na kondycji polskich firm należących do sektora MŚP, a coraz większe obciążenia na nie nakładane powodują, że ich głównym zmartwieniem często jest utrzymanie się na rynku. **Przyczyny niskiego poziomu inwestycji mają wiele wymiarów, jednak jednym z najważniejszych jest niestabilne prawo i niejasny system podatkowy. Konieczne są w tym zakresie fundamentalne reformy. Należy wprowadzić takie rozwiązania podatkowe, które sprzyjają modernizacji przedsiębiorstw, m.in. umożliwiając pełną i szybką amortyzację kosztów inwestycji w rozwiązania zwiększające cyberbezpieczeństwo (np. zakup oprogramowania, utrzymywanie serwerów itp.).**

[64] https://zpp.net.pl/wp-content/uploads/2023/02/09.02.2023-Busometr-Prognoza-na-pierwsze-polrocze-2023.pdf, (dostęp na dzień 08.11.2023 r.).

Rekomendacje

- **Pilnej modernizacji wymaga system kontroli ruchu pociągów. Biorąc pod uwagę integrację infrastruktury w ramach UE Polska z pewnością powinna wzorować się na istniejących rozwiązaniach i to nie tylko w zakresie ruchu kolejowego.**
- **USA posiada odrębną i na bieżąco aktualizowaną strategię cyberbezpieczeństwa przeznaczoną wyłącznie celom obronności. Tego rodzaju rozwiązanie nakierowane bezpośrednio na obronność byłoby w Polsce pożądane.**
- **Na szczeblu państwowym warto byłoby rozważyć wprowadzenie agencji podobnej do Israel National Cyber Directorate, która byłaby w stanie gromadzić dane o bezpieczeństwie cybernetycznym, monitorować zagrożenia i wymieniać informacje na szczeblu centralnym, a jednocześnie posiadałaby realne narzędzia do kreowania polityki cyberbezpieczeństwa państwa *ad hoc*. Pożądane byłoby również tworzenie jednostek podobnych do tajwańskiego „Team T5", które w sposób zorganizowany stałyby w pierwszym szeregu cybernetycznej wojny, walcząc z zagrożeniami.**
- **Należy wprowadzić takie rozwiązania podatkowe, które sprzyjają modernizacji przedsiębiorstw, m.in. umożliwiając pełną i szybką amortyzację kosztów inwestycji w rozwiązania zwiększające cyberbezpieczeństwo (np. zakup oprogramowania, utrzymywanie serwerów itp.).**

6. Podsumowanie

1. Jak wskazują liczne badania, Polska w zakresie cyberbezpieczeństwa oceniana jest stosunkowo dobrze. Wciąż bardzo daleko nam do liderów pod tym względem, niemniej jednak z pewnością można uznać nasz kraj za stosunkowo bezpieczny. Nie oznacza to oczywiście, że nie mamy się czym przejmować. W ostatnich latach dochodziło do wielu „spektakularnych" wpadek w tym zakresie, głównie na szczeblu instytucji publicznych, czy też firm państwowych obsługujących krytyczną infrastrukturę. Sytuacji z pewnością nie polepszają niepokoje geopolityczne, szczególnie wojna za naszą wschodnią granicą. Polska jako jedno z kluczowych państw dla zapewnienia wsparcia w konflikcie zbrojnym może być częstszym celem ataków hakerskich. Takie ataki zdarzają się już dziś i systematycznie rosną.
2. Nie tylko instytucje państwowe muszą zachować ostrożność. Również największe polskie firmy padały ofiarą cyberprzestępców, a jak pokazuje powołany przypadek ataku na CD Projekt Red, takie ataki mogą powodować bardzo poważne skutki mogące potencjalnie zagrozić nawet istnieniu firmy. Nie dziwi zatem, że jeśli ofiarami przestępców w sieci padają duże firmy inwestujące w bezpieczeństwo systemów znaczne środki, to niewielkie firmy należące do sektora MŚP obawiają się, że nie nadążą za zmieniającymi się na świecie wymogami w tym zakresie. Z całą pewnością wyzwaniem w najbliższych latach będzie poprawa sytuacji finansowej polskich przedsiębiorców tak, aby umożliwić im zwiększenie nakładów na inwestycje, w tym w cyberbezpieczeństwo. Aby dodatkowo zachęcić ich w tych działaniach stosunkowo prostym sposobem byłoby np. objęcie nakładów na bezpieczeństwo systemów informatycznych mechanizmem podobnym do ulgi na innowacje (na wzór ulgi na prototyp, robotyzację, czy B+R) i umożliwienie przedsiębiorcom odliczenia od podstawy opodatkowania 30 proc. kosztów związanych z wdrożeniem systemów cyberbezpieczeństwa w ich firmie. W ten sposób niewielkim kosztem zachęcilibyśmy przedsiębiorców do swego rodzaju profilaktyki zdarzeń niebezpiecznych, których koszt dla gospodarki może wielokrotnie przewyższać wartość udzielonej w ten sposób ulgi. Interesującym rozwiązaniem byłoby także traktowanie inwestycji w cyberbezpieczeństwo całościowo i umożliwienie przedsiębiorcom amortyzacji kosztów poniesionych na ten cel. Obecnie każdy z elementów takiej inwestycji musi być traktowany indywidualnie i w zależności od konkretnego przypadku może on podlegać amortyzacji bądź nie.

3. Rozwój Internetu i coraz powszechniejsze wkraczanie nowoczesnych technologii i sieci społecznościowych do naszego życia wymusza również ostrożność wśród internautów. W tym zakresie szczególnie ważne jest budowanie świadomości obywateli o istniejących zagrożeniach, gdyż największe niebezpieczeństwo powodowane jest przeważnie naszymi błędami, które często bardzo pomysłowo starają się wymusić oszuści. Utrata danych dostępowych do kont bankowych, czy włamania do „inteligentnych domów" są powszechnymi zjawiskami nie tylko w Polsce, ale w każdym rozwiniętym cyfrowo społeczeństwie.
4. Polska z pewnością powinna rozważyć budowanie prawdziwej, dobrze finansowanej strategii bezpieczeństwa wzorowanej na tych państwach, które już dziś zmagają się z największymi zagrożeniami. Warto rozważyć utworzenie agencji podobnej do Israel National Cyber Directorate, czy grup walki z atakami cybernetycznymi jak tajwański Team T5. Cyberbezpieczeństwo wymaga oczywiście również odpowiedniego finansowania, które powinno być traktowane na równi z bezpieczeństwem militarnym, gdyż w praktyce często te dwa zagadnienia są ściśle powiązane. Niestety nie możemy mieć złudzeń. Mimo że wciąż możemy mówić, że Polska jest stosunkowo bezpieczna, to wzrost naszego znaczenia gospodarczego, jak i politycznego, szczególnie w kontekście wojny na Ukrainie, będzie stale zwiększał nasze zagrożenie cybernetyczne. Prawdziwym wyzwaniem pozostaje zatem nadążenie za rosnącym niebezpieczeństwem.
5. Warto wskazać również na być może prozaiczny, ale w praktyce niezwykle ważny postulat. Jest to konieczność budowania świadomości o zagrożeniach cyfrowych w społeczeństwie. Pozwoli to nie tylko na ograniczenie ryzyka dla samych obywateli, ale także ułatwi ograniczenie go dla organizacji i instytucji państwowych, które wprost wskazują, że największe ryzyko często wiąże się właśnie z wykorzystaniem przez przestępców błędów ludzkich. Aby zrozumieć wagę tego postulatu wystarczy przyjrzeć się najpopularniejszym rodzajom ataków w Internecie, które opierają się w znaczniej mierze na manipulacji i socjotechnice.

Autorka składu:
Anna Śleszyńska

Zdjęcia: Canva.com

Użyto czcionek:
Poppins, Staatliches

Warsaw Enterprise Institute
Al. Jerozolimskie 30/7
00-024 Warszawa