Damian Białas
Imię i nazwisko
25528
Nr albumu
Bezpieczeństwo Narodowe
Kierunek:
Policja w systemie bezpieczeństwa publicznego
Specjalność:

Tryb: STACJONARNE / NIESTACJONARNE

O Ś W I A D C Z E N I E

Świadoma / świadom odpowiedzialności oświadczam, że przedkładana praca

licencjacka, inżynierska, magisterska* pt.:

PARADYGMAT CYBERPRZESTĘPCZOŚCI W ASPEKCIE ESKALACJI ZAGROŻEŃ BEZPIECZEŃSTWA NARODOWEGO

została napisana przeze mnie samodzielnie.

Jednocześnie oświadczam, że ww. praca nie narusza praw autorskich w rozumieniu ustawy z dnia 4 lutego 1994 roku o prawie autorskim i prawach pokrewnych (Dz. U. Nr 24, poz.83 z późniejszymi zmianami) oraz dóbr osobistych chronionych prawem cywilnym.

Ww. praca nie zawiera danych i informacji, które uzyskałam / uzyskałem w sposób niedozwolony. Niniejsza praca dyplomowa nie była wcześniej podstawą żadnej innej urzędowej procedury związanej z nadawaniem dyplomów wyższej uczelni lub tytułów zawodowych.

Oświadczam, że udzielam nieodpłatnie Akademii WSB prawa do wprowadzania i przetwarzania w systemie antyplagiatowym pracy dyplomowej mojego autorstwa.

Dąbrowa Górnicza, dnia 15.01.2023r. .....
Podpis

* odpowiednie podkreślić

Wydział Nauk Stosowanych
Kierunek studiów: Bezpieczeństwo Narodowe

PRACA DYPLOMOWA LICENCJACKA

Damian Białas

PARADYGMAT CYBERPRZESTĘPCZOŚCI W ASPEKCIE ESKALACJI ZAGROŻEŃ BEZPIECZEŃSTWA NARODOWEGO

Praca licencjacka
napisana pod kierunkiem
prof. AWSB dr. hab. Robert Socha

SPIS TREŚCI

Wstęp

Zjawisko postępującej cyfryzacji wśród społeczeństwa, jak i w jednostkach administracji publicznej, w zestawieniu z eskalującymi coraz bardziej przestępstwami w cyberprzestrzeni stanowi coraz większe wyzwanie w zakresie bezpieczeństwa narodowego Polski. To właśnie problematyka bezpieczeństwa Narodu Polskiego w cyberprzestrzeni stała się asumptem do napisania pracy dyplomowej. Stanowi ona bowiem asumpt do rozważań nad głębszymi problemami proceduralnymi i strukturalnymi systemu służb Bezpieczeństwa Narodowego. W związku z występowaniem problematyki powszechnej niewydolności organów służb policji, cyberpolicji i sądów w dobie eskalacji ilości występowalności cyberprzestępstw, zastosowano narzędzia w formie kwestionariusza wywiadu rozszerzonego o analizę narzędzi skali, a także własne doświadczenia z perspektywy ofiary cyberprzestępstwa. Omówiona zostanie sfera cyberprzestrzeni, zagrożeń które czyhają na nas w niej a także rozważone zostaną aspekty bezpieczeństwa naszych informacji wraz z securyzacją naszej sieci. Płaszczyzna cyber aspektów do poruszenia jest niesamowicie szeroka. Ukazany został sposób przedstawiający wiele elementów omawianego zjawiska, a także cyberprzestępczości, w tym opisu, aspektów prawnych, typologii i szereg problematyki związanej z nią. Niewątpliwie najgroźniejszym z punktu widzenia bezpieczeństwa jest cyberterroryzm który został ujęty w opracowaniu naukowym. Zagrożenia wynikające z cyberterroryzmu, spektrum działania, jak i bezpieczeństwo infrastruktury krytycznej i danych krajowych zostało opisane celem uświadomienia czytelnika z jak wielkim niebezpieczeństwem może wiązać się omawiana problematyka cyberprzestrzeni. Przedstawiona została w ujęciu technologicznym kwestia cyberbezpieczeństwa Rzeczypospolitej Polskiej a także bezpieczeństwo danych krajowych, w tym systemów operacyjnych i aplikacji oraz sprzętów. Ujęte zostaną również składowe sieci komputerowych a także czytelnik przekona się jakie były największe incydenty kradzieży krajowych danych przez cyberprzestępców. Ponadto podjęte zostały badania nad problematyką cyberprzestępczości w celu wykazania metodologicznych działań holistycznych, skłaniających się poprawie świadomości w zakresie cybersecurity, celem przyczynienia się do sprawniejszej organizacji instytucji a także redukcji zjawiska cyberprzestępczości. Omówione zostaną aspekty techniczne, prawne a także proceduralne. Dzięki poniższemu opracowaniu, czytelnik może wdrożyć się w

eksplorację obszaru cyberprzestrzeni, poznać zagrożenia płynące zeń a także dowiedzieć się, jakie metodyki działań przestępców są dziś spotykane najczęściej. Na koniec opracowania dokonana została konkluzja zjawiska przestępczości, wnioski wynikające z analizy przeprowadzonych badań wraz z materiałami, wywiadami eksperckimi a także opinią autora opracowania. Ów literatura może zatem stać się początkiem niezwykłej przygody ukierunkowanej na poznanie cyber-świata bliżej, w ujęciu technologicznym.

Rozdział 1. CYBERPRZESTĘPCZOŚĆ

Cyberprzestępczość w dzisiejszych czasach jest zjawiskiem które dzięki wyspecjalizowanym przestępcom, wykorzystuje obszary cyberprzestrzeni kuszące zasobami najbardziej pożądanymi przez sprawców w świecie przestępczym. Zjawisko to eskalując z roku na rok, powoduje iż skala zagrożeń i ryzyko stania się ofiarą, z coraz większym prawdopodobieństwem sięgnąć może zarówno nas jak i naszych bliskich.

1.1. Cyberprzestępczość – charakterystyka zjawiska

Cyberprzestępczość jest "zjawiskiem", które należy skategoryzować jako połączenie dwóch członów, cyber - neologizmu określanego jako sieci i obszary technologiczne w którym dokonywane są działania, oraz przestępczości wskazującej na czyn społecznie zabroniony. Definicja zjawiska cyberprzestępczości jest jednak trudna do zdefiniowania. Co do zasady cyberprzestępczość charakteryzuje użyciem technologii w obszarze cyberprzestrzeni, celem naruszenia dobra prawnie chronionego. Ze względu na swój charakter oraz formę naruszenia ów chronionego prawem dobra, dane przestępstwo określamy wedle szerokiej gamy terminologii zjawisk w cyberprzestrzeni. Termin cyberprzestępczość, w okresie początków rozwoju komputerowej technologii znany był pod terminem przestępczości komputerowej. Wedle pracy Dr. Hab. Macieja Siwickiego tj. "Podział i definicja cyberprzestępstw", Rainer von Zur-Mühlen jako pierwszy określił zjawisko przestępczości komputerowej jako "każde przestępcze działanie, w którym komputer stanowi albo narzędzie, albo przedmiot zamachu"[1]. Na skutek ewolucji przestępczości komputerowych w szerszym spektrum wykorzystywania systemów teleinformatycznych do nielegalnych celów, przyjęto z biegiem lat nową terminologię. Stosując neologizm "cyber" - określający zastosowanie w systemie teleinformatycznym gdzie połączono ów człon z zestawieniem przestępczości. Tak powstałe określenie cyberprzestępczości po raz pierwszy użyte zostało tuż po nastaniu drugiego millennium. W 2001 roku bowiem fakt wejścia w życie ustanowionej przez Radę Europy Konwencji o cyberprzestępczości", sprawił iż wzmianka terminologiczna stała się asumptem do używania słowa cyberprzestępczość w nazewnictwie. Od tegoż momentu termin ten był stosowany w wielu innych artykułach. Ustanawiającym stricte definicję cyberprzestępczości jest jednakże wzmianka Komunikatu Komisji

[1]s M. Siwicki *Podział i definicja cyberprzestępstw, Materiały Szkoleniowe*, [b.m.w], 2012, s. 242.

Europejskiej nr 267 z 2007 r. w którym określono ów zjawisko jako „czyny przestępcze dokonane przy użyciu sieci łączności elektronicznej i systemów informatycznych lub skierowane przeciwko takich sieciom i systemom”[2]. Termin ten wielokrotnie przytaczano w kolejnych dokumentach dzięki czemu ów termin został sukcesywnie przyjęty za właściwy w odniesieniu do definicji zjawiska. Cyberprzestępczość przytaczała iż realizowana mogła być w obszarze cyberprzestrzeni. Przestrzeń ta, ulokowana w świecie cyfrowym stanowi wirtualny obszar teleinformatyczny o ogromnych zasobach danych. Istnieje ona dzięki sukcesywnym rozwoju myśli technologicznej w sektorze teleinformatyki, pozwalającej użytkownikom na operowanie dzięki uprawnieniom, w określonej części cyberprzestrzeni. Wiedza przestępców w zakresie technologicznej struktury poszczególnych systemów oraz umiejętności obejścia zabezpieczeń, stanowić może istotne zagrożenie dla bezpieczeństwa umieszczonych w nim danych. Wraz z rozwojem myśli technologicznej, tworzonymi zabezpieczeniami oraz usprawnieniami w obszarze teleinformatycznym w myśl akcji - reakcji przestępcy stale doszukują się luk i płaszczyzn w obszarze cyberprzestrzeni, celem dokonania przestępstwa. Sugerując się Komunikatem Komisji do Parlamentu Europejskiego, Rady oraz Komitetu Regionów, zauważyć można iż określone są trzy definitywne typy cyberprzestępstw. Najpopularniejsza forma cyberprzestępstwa w dobie dzisiejszych czasów czyli oszustwo oraz fałszerstwo są określane mianem tradycyjnej formy przestępstwa jednakże popełnionej za użyciem systemów i elektronicznych sieci informatycznych. Kolejną formą jest przestępstwo polegające na opublikowaniu treści nielegalnych w obszarze cyberprzestrzeni kodowanych cyfrowo, najczęściej w formie binarnej. Treści te odczytywane mogą być za pomocą urządzeń elektronicznych. Za przykład, przytoczyć można seksting, treści o charakterze nawołującym do przemocy, nienawiści czy pedofilii. Ostatnią z form przestępstw określonych w komunikacie Komisji nr. 267, są przestępstwa skierowane w stronę systemów teleinformatycznych. Wśród nich możemy określić np. ataki hakerskie łamiące zabezpieczenia, denial of service blokujące dostęp do systemu teleinformatycznego. Zjawiska o powyższych charakterach mają zastosowanie często w przypadku ataków na najważniejsze systemy infrastruktury krytycznej danego kraju. Ogromne niebezpieczeństwo powyższych ataków charakteryzuje skala z jaką mogą zaszkodzić kluczowym systemom w poszczególnych krajach. Skuteczny atak może ze

[2] Komunikat Komisji do Parlamentu Europejskiego, Rady oraz Komitetu Regionów z dnia 22.5.2007, Kom(2007) 267 wersja ostateczna, 2007, Bruksela.

znacznych odległości, zdalnie uszkodzić wiele danych a także zaburzyć procesy kooperacji służb w wybranych obszarach co doprowadzić by mogło do ogromnych szkód dla poszczególnych Państw, służb lub organizacji. Możliwość zdalnego dokonywania przestępstwa, dające dodatkowy czas na reakcję oraz realizację jego procesu jest jednym z asumptów zachęcających przestępców do realizacji przestępstwa w cyberprzestrzeni. Istota możliwości dokonywania przestępczości komputerowej bez fizycznej obecności oraz przy uwzględnieniu ryzyka poniesienia niższych sankcji karnych w zastosowaniu systemu prawnego wobec przestępcy, przyciąga coraz to nowe zorganizowane grupy przestępcze a także indywidualnych cyberprzestępców do cyber-świata. Wizja poniesienia mniejszych konsekwencji prawnych względem fizycznego wykonania podobnego przestępstwa z pewnością jest motywującym czynnikiem wśród przestępców przenoszących się do cyberprzestrzeni.

Zjawisko przestępczości obecne jest od zarania dziejów. Odkąd ustalono system porządku społecznego, przejaw niesubordynacji wobec niego łamał zwyczajowe normy . Już w 2360 roku p.n.e. Król Urukaginy, Lagasz zastosował system prawny w swoim mieście. Ów regulacje systemu prawnego miały charakter imperatywny, narzucający reguły pożądanych zachowań oraz karzący te, odbiegające od nakazanych norm. W XVIII wieku p.n.e. najsłynniejszy król z pierwszej dynastii Babilonu, syn i następca Sin-muballita stworzył surowy, aczkolwiek stanowczy Kodeks, zwanym od imienia władcy Kodeksem Hammurabiego. Powyższe rygorystyczne prawo, docelowo stworzone było celem podporządkowania obywateli i redukcji poszczególnych zjawisk społecznych a także przestępstw w sposób kazuistyczny. Przejaw przestępczości w średniowieczu zaś, uznawany był bowiem za dzieło wysłannika szatana na ziemi. Ówczas czyny przestępcze karano śmiercią. Wraz z biegiem historii, honorowano prawa Mojżeszowe opisane w księdze Exodus w zestawieniu z prawem miejscowym, zaś w czasach nowożytnych ewolucja poszczególnych systemów prawnych w postaci konstytucji i systemów prawnych niższego szczebla rozwinęła się, obiegając cały cywilizowany świat. Wraz z rozwojem systemu prawnego, postępowała metodyka działania przestępców. Niemniej wspólnymi cechami przestępstw na przestrzeni dziejów w ujęciu historycznym są trzy najważniejsze składowe. Pierwszą i najważniejszą jest fizyczny udział przestępcy w procesie dokonania przestępstwa. Kolejną składową jest przynależność do określonej w danej epoce historycznej grupy społecznej. Ostatnią zaś jest odniesienie się do autorytarnych wartości nadanych od

istoty Boskiej, stąd każdorazowe złamanie powyższych reguł stanowiło przejaw naruszenia religijnego porządku rzeczy[3]. Nasuwa się na myśl stwierdzenie iż wraz z rozwojem i egzekucją prawa pisanego na przestrzeni dziejów, sprawczość przestępcza ewoluowała i wraz ze zmienianym prawem, zmieniała sposoby dokonania przestępstw by stać się nieuchwytnym i osiągać zamierzone przez siebie, lecz niezgodne z prawem cele. Rozwój przemysłu oraz komputerów na którym można było zachować informacje w formie binarnej stworzył nowe spektrum możliwości dla wyspecjalizowanych technologicznie przestępców, co miało niebagatelny wpływ na bezpieczeństwo użytkowników systemów teleinformatycznych. Po raz pierwszy w historii przestępcy mogli zacząć dokonywać przestępstwa w świecie wirtualnym, często z dowolnego miejsca na ziemi. Dzięki znajomości technologii a także użyciu programów, dokonanie przestępstwa w cyberprzestrzeni stało się o wiele łatwiejsze dla sprawców. Nieuwaga, brak przezorności w zapewnieniu bezpieczeństwa oraz uśpiona czujność sprawia że przestępcy coraz śmielej i częściej dokonują cyberprzestępstw[4] Biorąc pod uwagę mniejsze ryzyko bycia złapanym przez organy ścigania, potencjalnie skuteczniejszą możliwość zbudowania "siatki przestępczej i komunikacyjnej" oraz zmniejszony poziom czujności ofiar i niższe konsekwencje prawne, całokształt zjawiska przyczynia się do znacznej tendencji wzrostu ilości cyberprzestępstw.

1.2. Wielopłaszczyznowe zagrożenia cybernetyczne

Gama zagrożeń we współczesnym świecie cybernetycznym nieustannie się zmienia. Wynika to w szczególności z eksplorowania podatności infrastruktury teleinformatycznej na ataki przez osoby nieuprawnione do ingerencji w dostęp danego systemu, sieci lub danych. Zabezpieczenie danych swojego systemu w stu procentach jest w gruncie rzeczy niemożliwe. Wynika to z faktu iż wówczas dostęp do systemu musiałby zostać uniemożliwiony przez jakiegokolwiek użytkownika. Co więcej, ów system musiałby być odłączony stale od sieci. Niepraktyczność tego rozwiązania sprawia że użytkownik jakiegokolwiek systemu informatycznego, zobligowany jest do zastosowania środków zabezpieczających przed potencjalnym atakiem ze strony cybernetycznego środowiska. Mając na uwadze możliwość wystąpienia niepożądanego dostępu do cyfrowych danych swojego urządzenia, należy zastosować szereg czynności

[3] A. Juszczak, *Rys Historyczny Przestępczości, [w:] Security, Economy & Law Nr 1/2018 (XVIII), (74–85) DOI 10.24356/SEL/18/4 , s. 75.*
[4] Źródło: Nask, https://www.nask.pl/pl/aktualnosci/4266,CERT-Polska-informuje-o-znacznym-wzroscie-liczby-oszustw-komputerowych.html z dnia 20.06.2022 r.

zabezpieczających przed osobami nieuprawnionymi do ich eksploracji. Ogrom rodzaju zagrożeń w cyberprzestrzeni stanowi wyzwanie dla zabezpieczających programistów wyzwanie, jednakże wymienić możemy najczęstsze z występujących ataków.

Najpopularniejszym od lat określeniem osoby łamiącej owe zabezpieczenia, uzyskującej dostęp do sfery cyberprzestrzeni z chronionymi cyfrowymi danymi jest Haker. Określenie to jest przypisane osobie która swymi umiejętnościami łamiącymi zabezpieczenia dokonała tzw. Hackingu. Z definicji Hacking jest nieautoryzowanym dostępem do chronionego systemu teleinformatycznego służącym do wykradania danych z systemu, celowym prosperowaniem łamiącym szyfrowanie zabezpieczeń poprzez modyfikację zasobów lub implementację służących do tego wirusów. Na niebezpieczeństwo te narażeni mogą być wszyscy użytkownicy sprzętów elektronicznych. Zarówno zabezpieczenia rządowe, korporacyjne systemy gromadzące dane jak i przeciętni użytkownicy nie mający zabezpieczającego, choć nie na wszystkie ataki - oprogramowania przeciwwirusowego. Skutki skierowanego na poszczególną jednostkę ataku hakerskiego mogą być kosztowne w skutkach. Uzyskując dostęp do systemów lub sieci informatycznych, bystry Haker jest w stanie wykraść nasze dane, ujawnić tajemnice rządowe, korporacyjne a także całkowicie je zmodyfikować dokonując zaszyfrowania plików, żądając za ich odszyfrowanie okupu. W związku z powyższym pozostaje również Cracking jako forma przełamania zabezpieczeń danego oprogramowania w celu osiągnięcia materialnych korzyści. Tego typu forma crackowania danych przez przestępców zwanych Crackerami, niemal w każdym przypadku używana, przełamuje zabezpieczenia łamiąc licencje crackowanego oprogramowania. Cracking jest działaniem służącym do przełamywania technicznych zabezpieczeń, obchodzenia ich a także przechowywania i nielegalnego zwielokrotniania zasobów danego oprogramowania[5]

Programiści tworzący skomplikowane oprogramowania a także systemy czy aplikacje, w celu zdalnego obejścia zabezpieczeń i modyfikacji kodu w którym dane oprogramowanie powstało, tworzą luki typu backdoor. Owa furtka wyłapana przez osobę nieuprawnioną do ingerencji w oprogramowanie pozwala na obejście jego

[5] Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych Art. 118. ust. 1, ust. 2.

zabezpieczenia. Backdoor jest specyficznym rodzajem cyberzagrożenia które przy znajomości określonego języka programowania danych, daje możliwość wykorzystania w sposób nieautoryzowany ten kanał dostępu. Znajomość luki oraz języka napisanego oprogramowania, sprawca ataku może dokonać znaczących szkód technicznych. Takowy dostęp pozwala na całkowite uniemożliwienie funkcjonowania oprogramowania, jego modyfikację poprzez umieszczenie złośliwego trojana a także na zdalne kontrolowanie urządzenia ofiary.[6]

Jedną ze sprytnych form uzyskiwania dostępu do danych przez hakerów jest metoda Sniffingu. Ten rodzaj zagrożenia z perspektywy użytkownika sprzętu teleinformatycznego jest równie niebezpieczny co powyższe ataki. Sniffing charakteryzuje się "podsłuchiwaniem" informacji przesyłanych między urządzeniami celem wychwytywania poszczególnych wrażliwych danych w tym głównie loginów, haseł, treści wiadomości a także ruchu teleinformatycznego.[7]

Coraz szerzej znanym przejawem zjawiska cyber-przestępstwa w sieci na całym świecie są ataki Spoofingu. To swego rodzaju pozorne podszycie się pod określoną osobę, instytucję, firmę lub jednostkę mające na celu oszukanie ofiary celem wykorzystania jej zaufania i zdobycia poufnych danych. Spoofing może być sukcesywnie wykorzystywany przez przestępców w wielu obszarach technologicznych. Począwszy od podszywania się pod domeny fałszywych stron, numery telefonów instytucji bankowych czy jednostek służb. Tego typu operacja służyć ma temu by oszukać potencjalną ofiarę, nakłonić ją do podania poufnych danych a także często to dokonania operacji finansowych.

Od zarania komputerowej rewolucji, wraz z możliwością implementacji nowego oprogramowania, przez wprawnych cyberprzestępców tworzone są również złośliwe oprogramowania mające ingerować w nie. Hakerzy tworząc wirusa, mogą mieć wiele różnych motywacji. Manifestacja poglądów, zaprezentowanie swoich umiejętności łamania zabezpieczeń, uzyskaniem dostępu do danych, ich kradzież lub uszkodzenie. Co do zasady jednak wirusy mogą stanowić poważne niebezpieczeństwo dla urządzeń które są nimi zainfekowane. W zależności od budowy szkodliwego oprogramowania, poprzez multiplikację, są w stanie zainfekować zarówno jedno, jak i wszystkie

[6] Z. Danielewicz, *Zeszyty Naukowe Wydziału Elektroniki i Informatyki Politechniki Koszalińskiej,* Koszalin, 2018, Nr 13,s. 48-49

[7] S. Mazur, *Zagrożenia bezpieczeństwa danych w lokalnych sieciach komputerowych – ataki i metody obrony*, Karkonoska Państwowa Szkoła Wyższa w Jeleniej Górze, Jelenia Góra, [b.r.w.], s. 1.

urządzenia podłączone do sieci. Wartym wspomnienia jest tutaj wirus KLEZ który w przeciągu 2,5 godziny zainfekował cały ówczesny internet. Spektrum zagrożenia dopełnia fakt iż wirusy te mogą przejąć kontrolę nad komputerem, wydobyć poufne informacje a także przeciążyć łącza uniemożliwiając skuteczną komunikację.

Jednym z najbardziej znanym w ówczesnych czasach sposobem dokonania przestępstwa w cyberprzestrzeni jest phishing. Podobnie jak w przypadku bardziej zaawansowanego technologicznie Sniffingu, celem ataku jest użycie narzędzi socjotechniki, wprowadzenie ofiary w błąd i finalnie dokonując podszycia się pod zaufaną osobę, stronę internetową czy instytucję celem osiągnięcia korzyści materialnych lub kradzieży poufnych danych. Dzięki inżynierii społecznej, atakujący wykorzystując metodykę strachu, zaufania lub wykorzystując chciwość ofiary, przekonują ją do wykonania określonych czynności. Ich następstwem, prócz utrata danych wrażliwych czy finansów, może być również udostępnienie możliwości sprawcy, dostępu do systemów o wyższym poziomie tajności, w tym instalację lub uruchomienie koni trojańskich. Niebezpieczeństwo zniszczenia, uszkodzenia lub kradzieży danych jest tym większe, im bardziej strzeżone systemy poprzez użycie narzędzi socjotechnicznych atakujący ominie. Skuteczna forma zabezpieczenia sprzętu komputerowego przed uszkodzeniami, stratami materialnymi, wyciekiem wrażliwych informacji lub całkowitą utratą danych jest trudna, lecz nie niemożliwa. Ochrona urządzenia przed atakami hakerskimi bądź też zautomatyzowanym systemem atakującym sprowadza się w gruncie rzeczy do ochrony systemu za pomocą wbudowanej, aktualizowanej na bieżąco zapory systemu operacyjnego, korzystaniem z rozbudowanych oprogramowań antywirusowych a także zachowaniem ścisłej procedury bezpieczeństwa[8]. Powyższe składowe mają się jednak na nic w przypadku gdy wykorzystywane są przez atakującego luki w oprogramowaniu i procedurom, które jeszcze nie są znane twórcom. Efektem częstej specyfiki łatania luk w oprogramowaniu jest fakt iż twórcy łatają je w momencie gdy zostanie ono wykryte metodą “in-vivo” na gotowym produkcie. O ile producenci finansują badania nad oprogramowaniem przez testerów, to jednak nie wszystkie uchybienia mogą zostać wyłapane. Dlatego tak ważnym jest by jak najskrupulatniej dopracować środowisko bezpieczeństwa oprogramowania na którym użytkownik będzie operować.

[8] M. Szeliga, *Certyfikowany Specjalista IT Security,* Kwidzyn, 2015, s. 81-85.

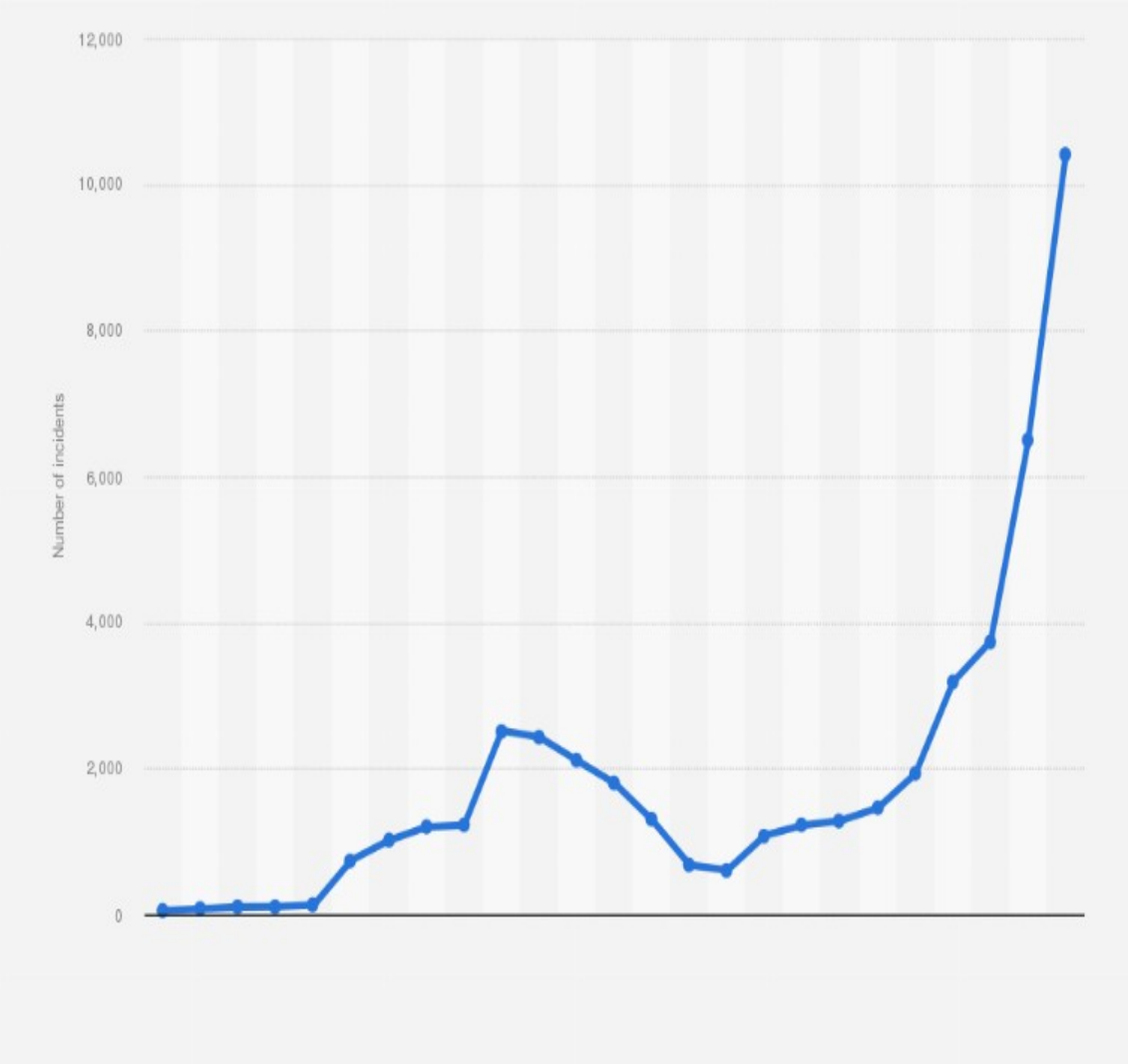
Cybernetyczny świat jest ciągłą zmienną, zarówno pod względem technologicznym, jak również w ujęciu przestępczym. Wynika to ze stałego rozwoju architektury oprogramowań a także dostępności stosowania coraz to nowych narzędzi jakimi posługują się programiści. W ujęciu cyberprzestępczości, istotnym elementem jest skutek jaki sprawca zamierza osiągnąć. Wspomniane wcześniej motywy przestępcy operującego w cyberprzestrzeni mają istotną rolę w pojęciu trendu ewolucji działań przestępców na tle cybernetycznym. Hakerzy prezentujący swoje umiejętności łamania zabezpieczeń to nieliczna grupa specjalistów, którzy operują zazwyczaj w sposób ideologiczny. Są to głównie aktywiści działający w obronie wolności, sprzeciwu wobec korupcji, nadmiernemu konsumpcjonizmowi czy cenzurze. Dokonując przejęcia danych, dokumentów czy list osób, ukazują je światu. Najbardziej znanym zespołem Hakerów o tym charakterze jest grupa Anonymous. Wstrząsając swoimi umiejętnościami cały świat, porusza istotne problemy społeczne, cyfrowo przeciwdziała nieuczciwym praktykom, w imię idei. Za największą z przeprowadzonych przezeń akcji hakerskich, można uznać obronę WikiLeaks[9]. Ów strona służąca do anonimowego publikowania tajnych, rządowych a także korporacyjnie ważnych treści, powstała celem ujawnienia nieuczciwego działania firm i osób powiązanych z publikowanymi informacjami. Celem przeciwdziałania wyżej wymienionej grupy sygnalistów była protekcja tejże strony, by swymi działaniami hakerskimi, powstrzymać łamiących prawo i zasady moralne.

Udoskonalane techniki tworzenia architektury oprogramowania postępuje wraz z coraz nowocześniejszymi technologiami. Wraz z powyższymi dwoma czynnikami, a także dzięki znajomości luk w oprogramowaniu, powstają coraz to bardziej skomplikowane wirusy mogące złamać zabezpieczenia. Trend ten przyspieszył w ostatnich latach. Co roku zwiększa się ilość incydentów ataków Od roku 1996 do 2020-go wskaźnik statystyki występowalności ataków w cyberprzestrzeni, z kilkuletnią bessą rośnie. Bowiem z 50 przejawów incydentu w roku 1996, ilość ta zwiększyła się do 10,420 w roku 2020-tym. Statystyki te przejawiają gwałtowny wzrost od roku 2011-go w którym to przekroczyły już ilość kilkuset, z czego w latach kolejnych nastąpiła eskalacja przestępstw na płaszczyźnie cybernetycznej. Drastyczny wzrost występowalności incydentów cyberprzestępstw w Polsce w ostatnich dekadach, sugerować może iż trend ich dokonywania nie w wymiarze fizycznym, lecz wirtualnym.

[9] Źródło; Wikipedia, https://pl.wikipedia.org/wiki/WikiLeaks, z dnia 27.06.2022 r.

Powyższe wnioski przedkładając się wskazują iż departamenty ds. walki z cyberprzestępczością są segmentem którego zasilenie dodatkowymi środkami z budżetu Państwa będzie istotne w kolejnych latach.[10]

Wykres 1. Liczba incydentów cyberbezpieczeństwa obsłużonych przez CERT* w Polsce w latach 1996-2021



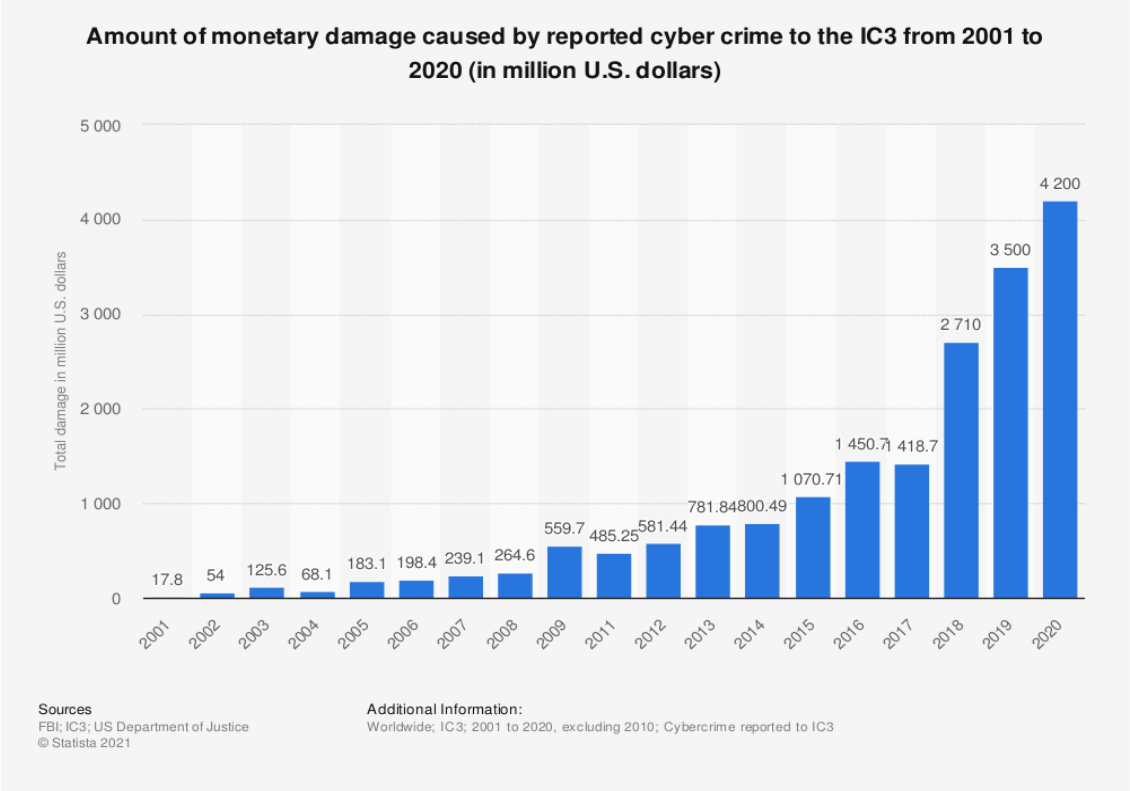
Źródło: Statcdn, https://cdn.statcdn.com/Statistic/1025000/1028557-blank-754.png z dnia 28.06.2022 r.

Ekstrapolując od powyższych statystyk sugerujących coraz częstszą eksplorację przez przestępców świata wirtualnego, wydaje się być zasadnym iż chcąc uzyskać coraz to większe zyski ze swojego cyber-przedsięwzięcia, obierają skalowalny trend sektora finansowego. Powyższe dopełniają statystyki FBI ukazujące wolumenowy wzrost strat zaatakowanych ofiar w latach 2001-2020. Skalowalny i finansowy motyw ataków

[10] Źródło; Statista, https://www.statista.com/statistics/1028557/poland-cybersecurity-incidents/ z dnia 28.06.2022 r.

obrany przez cyberprzestępców jest zauważalny, mniej więcej w korelacji do ich ilości w ostatniej dekadzie.

Wykres 2. Kwota szkód pieniężnych wyrządzonych przez zgłoszone cyberprzestępstwa do IC3 w latach 2001-2020 (w milionach dolarów amerykańskich)

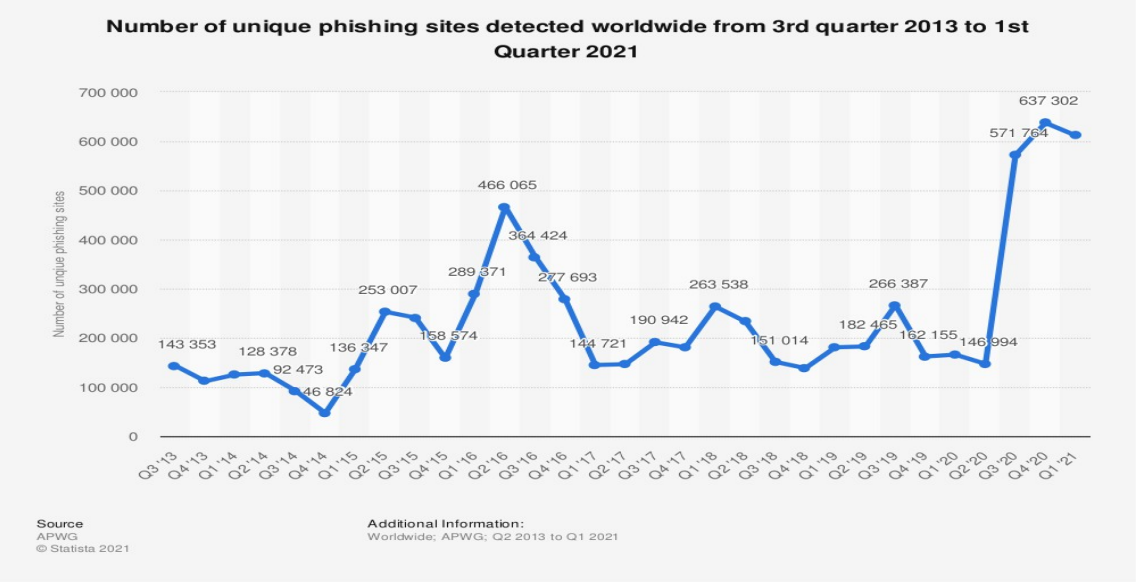


Źródło: Statista, https://www.statista.com/graphic/1/267132/total-damage-caused-by-by-cyber-crime-in-the-us.jpg z dnia 28.06.2022 r.

W ostatnich latach wróciła do łask choć niebezpieczna, to wykorzystująca podstawowe filary socjotechniki Phishingowa forma ataku. Targetowana na wrażliwe dane jak i finanse metoda, od drugiego kwartału 2020-go roku stała się najbardziej rozpowszechnionym zagrożeniem w cyberprzestrzeni. W zbiegu korelacji z ogłoszoną ogólnoświatową pandemią Covid-19, cyberprzestępcy stosując umiejętnie techniki manipulacji socjotechnicznych dokonali wzmożonych ataków zarówno na cywili, pracowników firm z sektora prywatnego, jak i urzędników państwowych. Jak wynika ze statystyk, środowisko w którym w związku z sytuacją pandemiczną nastąpiła konieczność komunikacji, organizacji spraw finansowych jak i służbowych zdalnie, sprawiło iż przestępcy stali się bardziej aktywni w cyberprzestrzeni. Na przełomie pierwszego i drugiego kwartału 2020-go roku, ilość założonych i funkcjonujących

domen które zostały zaraportowane jako phishingowe wzrosła liniowo. W okresie od drugiego do czwartego kwartału, ilość ta wzrosła ponad czterokrotnie, sugerując tym samym iż Phishing stał się polem eksploracji cyberprzestępców. Prócz powyższych założeń, jak wynika z Raportu ZBP - 81% ankietowanych, wychodzi z założenia iż to Bank ponosi odpowiedzialność za bezpieczeństwo finansowych usług elektronicznych. [11] Uśpiona czujność, a także nadmierne zaufanie do usług z których użytkownik korzysta, może stać się asumptem do bycia celem ataku cyberprzestępców. Przekładając powyższe rozważania na grunt społeczny, czynniki psychologiczne oraz brak skrupulatnie sprawdzanych domen, odnośników czy wiadomości, przyczynia się do zwiększenia ilości skutecznych ataków. Jak donosi kom. Dominik Rozdziałowski, Dyrektor ds. walki z cyberprzestępczością Komendy Głównej Policji podczas konferencji CyberGov 2018 w Warszawie, tworzone zostają wręcz zorganizowane grupy przestępcze, wykradające w myśl skalowalności, coraz większe ilości danych oraz finansów obywateli.

Wykres 3. Liczba unikalnych stron phishingowych wykrytych na całym świecie od 3. kwartału 2013 r. do 1. kwartału 2021 r.

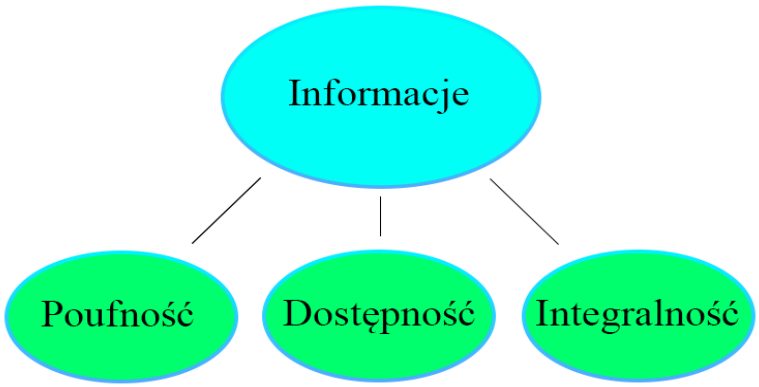


Źródło: Statista, https://www.statista.com/statistics/266155/number-of-phishing-domain-names-worldwide/ z dnia 30.06.2022 r.

By przedstawić istotę bezpieczeństwa informacji i systemów teleinformatycznych, należy zdefiniować czym owe bezpieczeństwo w ujęciu

[11] Związek Banków Polskich, *Raport ZBP Cyberbezpieczny portfel,* Edycja III, 2020 r, s. 6.

cybernetycznym jest. W ujęciu Cambridge Dictionary of English jest to *Zdolność do unikania szkód będących wynikiem dowolnego ryzyka, niebezpieczeństwa lub zagrożenia.* Zważywszy na szybkość postępu technologicznego, zasadnym wydaje się założyć iż nie jesteśmy bezpieczni. Oprogramowania zabezpieczające systemy teleinformatyczne, stanowią jedynie część zapory przed przestępcami chcącymi w nieuprawniony sposób dostać się do danych. Zatem to po stronie użytkownika leży między innymi zastosowanie pewnych form proceduralnych zabezpieczeń. Wynika stąd iż istota bezpieczeństwa informacji staje się procesem prowadzącym do zabezpieczenia i stałego czujnego monitorowania systemu teleinformatycznego. Normy Polskie w aspekcie bezpieczeństwa informacji definiują iż winny one być przechowywane na trzy poniższe właściwości.



Rys. 1 Właściwości bezpieczeństwa informacji

Źródło: Materiał graficzny autorstwa własnego

Poprzez ograniczenie uprawnień użytkownikom danego urządzenia, możemy ograniczyć dostępność i zapewnić poufność informacji. Czy zatem zapewnienie poufności jest wystarczające? Otóż okazuje się że nie. Sama restrykcja jest dość ryzykowna gdyż w przypadku utraty klucza bez zastosowania kopii zapasowej danych, spowoduje nieodwracalną ich utratę. Kolejnym elementem składowym bezpieczeństwa informacji jest ich integralność. Polega ona na dokonaniu zmian w zabezpieczeniu informacji w sposób, by ograniczyć możliwość ich eksplorowania a także przeszyfrowania. Ostatnią częścią dopełniającą poprzednie dwie składowe bezpieczeństwa informacji jest dostępność. Z oczywistych względów, nie można zapewnić absolutnej dostępności do danych w trybie ciągłym.

Zwiększenie dostępności usługi np. z 99% na 99,9% jest niezmiernie trudne i bardzo kosztowne zaś jej wzrost automatycznie sprawia iż poziom bezpieczeństwa w aspekcie poufności i integralności informacji maleje. Wynika z tego iż w zależności od potrzeb danego administratora danych, należy bardzo gruntownie, w sposób analityczny oszacować ryzyko i możliwości jego wystąpienia. W następstwie powyższych czynności, powinno się opracować procedurę bezpieczeństwa przepływu informacji, przeszkolić osoby użytkujące o możliwościach ataku z użyciem metod socjotechnicznych a także wdrożyć szereg metod zabezpieczenia informacji i danych. Rola informacji jest kluczowa do osiągnięcia zamierzonych celów w wielu aspektach życia społecznego czy zawodowego. Uzyskane przez nieuprawnioną osobę informacje o loginach i hasłach, mogą przyczynić się do utraty prywatności, danych a najgorszym przypadku środków z banku i ściśle strzeżonych tajemnic, czy to handlowych, czy rządowych. Strzeżenie ich jest więc ważnym elementem operowania na systemach teleinformatycznych. W zabezpieczaniu informacji, ze szczególnym wyzwaniem mierzą się administratorzy baz danych. W celu zapewnienia maksymalnej ich poufności ich sklasyfikowanie powinno się opierać na kategoryzacji wedle poziomu dostępności. Klasyfikację danych rozdzielamy na:

- publiczne - czyli dane które będąc ogólnodostępnymi, nie spowodują szkód, zaś zastosowanie poufności wobec nich nie jest konieczne.
- prywatne - czyli dane określone w ustawie o ochronie danych osobowych nad którymi czuwa Generalny Inspektor Ochrony Danych Osobowych. Tego typu dane pozwalają na zidentyfikowanie osób, zatem ich udostępnienie wymaga zgody na ich przechowywanie a także przetwarzanie,
- wrażliwe - czyli Prywatne dane które osób których dotyczą winny być objęte nadzorem i ochroną gdyż ich wyciek wiązać się wiązać z narażeniem na poniesienie przez te osoby szkód,
- tajne - Czyli dane najwyższego priorytetu securyzacji. Wśród nich wymienić możemy hasła, loginy, ściśle pilnowane tajemnice handlowe, państwowe. Dostęp do nich powinien być bardzo ograniczony do osób zaufanych a każdorazowe użytkowanie tajnych danych, należy nadzorować i monitorować. Ujawnienie tego rodzaju danych może doprowadzić do opłakanych następstw,

Stosowanie rozwiązania kategoryzacji i stopniowania ważności danych jest jedną z procedur która jest podwaliną do wprowadzenia kolejnych zabezpieczeń

poszczególnych kategorii. Należy jednak pamiętać by stosowane rozwiązania były ściśle przestrzegane a monitorowanie zabezpieczeń tych kategorii było regularnie, a w przypadku wykrycia luki bezpieczeństwa, na bieżąco aktualizowane.

Istotnym elementem zarządzania informacjami w cyberprzestrzeni jest możliwie jak najdokładniejsze zgłębienie środowiska teleinformatycznego w którym się operuje. Zasadnym jest to tym bardziej iż w przypadku ataku hakerskiego, kluczowa jest natychmiastowa reakcja administratora w protekcyjnym operowaniu proceduralnym. Znajomość środowiska którym się operuje, sprawia iż administrator bazy danych za których zabezpieczenie odpowiada, uzyskać może przewagę nad osobą nieuprawnioną chcącą się do niej włamać. Ponadto ważnym przy przechowywaniu danych, jest stosowanie się do normy BS 7799 wedle której to istotnymi elementami dziesięciu zakresów zabezpieczeń są kolejno wg poniższych zakresów zabezpieczeń uwzględnionych wg. norm BS 7799. Przedstawiają one obszary w których priorytetowo winny być poczynione starania w implementacji zabezpieczeń. Kolejno są to[12] :

1. Polityka bezpieczeństwa.
2. Organizacja bezpieczeństwa.
3. Klasyfikacja i kontrola aktywów.
4. Bezpieczeństwo osobowe.
5. Bezpieczeństwo fizyczne i środowiskowe.
6. Zarządzanie systemami i sieciami.
7. Kontrola dostępu do systemu.
8. Rozwój i utrzymanie systemu.
9. Zarządzanie ciągłością działania.
10. Zgodność.

W celu podjęcia podstawowych działań prewencyjnych zmierzających do zminimalizowania ryzyka uszkodzenia lub utraty danych, istotnym jest stosowanie podstawowej zasady ostrożności i ograniczonego zaufania. Jak wynika z analizy ilości powstawania domen phishingowych, sugeruje ona iż ilość zjawisk phishingu jest coraz powszechniejszą formą ataku na dane i finanse użytkowników sieci teleinformatycznej.[13] W dobie uśpionej czujności i globalnej cyfryzacji, narażeni jesteśmy na ryzyko stania się ofiarą cyberprzestępców stosujących socjotechniczne

[12] W. Dworakowski, *Zarządzanie bezpieczeństwem informacji wg normy BS 7799 – Wprowadzenie*, Kościelisko, 2005, s. 191.

metody wywierania wpływu i presji celem uzyskania dostępu do wrażliwych danych. Tym samym dochodzimy do konkluzji iż najsłabszym ogniwem całego systemu zabezpieczeń potencjalnie staje się człowiek. Zdecydowana większość osób nie zna technicznych aspektów systemów teleinformatycznych zatem koniecznym jest uświadomienie użytkownikom systemu o powyższych zagrożeniach, metodyczne przeszkolenie ich, by przygotować użytkowników do podjęcia stosownych działań proceduralnych w przypadku wystąpienia próby phishingu. Proces przygotowania pracowników na potencjalne ataki phishingowe, wykorzystujące ludzką naturę, może ograniczyć negatywne skutki wycieku danych a także finansów. Kolejnym ważnym elementem zabezpieczenia naszych wrażliwych danych, jest wypracowanie w sobie nawyku każdorazowego sprawdzania wysyłanych do nas wiadomości, maili czy też połączeń telefonicznych. Ilość metod prowadzonych wyłudzeń jest multum. Jednakże w przypadku uzyskania wiadomości sugerującej np. niedopłatę na kwotę "X" złotych u operatora komórkowego, zanim dokonamy jakiejkolwiek ingerencji klikając w link, sprawdzić należy w pierwszej kolejności czy ów wiadomość dotarła z oficjalnego kanału kontaktowego usługodawcy. W sytuacji gdy otrzymujemy podejrzaną wiadomość nietypowym kanałem komunikacji po raz pierwszy, należy skontaktować się usługodawcą podejmując oficjalną formę komunikacji celem wyjaśnienia sytuacji. Jako iż często w podejrzanych wiadomościach, komunikatorach czy też mailach wysyłane są również linki, ważnym jest, by sprawdzić czy protokół szyfrujący będący przedrostkiem do strony www, jest formą zabezpieczającą nasze dane, czy też nie. Https jest bezpieczniejszą formą szyfrującą nasze dane, zaś Http już niestety nie. Ponadto sprawdzić należy w adresie linku czy nie znajdują się tzw. "literówki" np. https://www.lng.pl/ zamiast https://www.ing.pl/ . W pierwszym linku zauważyć można podmienioną literę "i" na literę "l' co podczas wstępnej analizy wiadomości pozwoli nam stwierdzić iż jest to fałszywa wiadomość phishingowa. Mimo wszystko warto skontaktować się dodatkowo z dostawcą usługi której wiadomość dotyczy gdyż cyberprzestępstwa są dokonywane na coraz bardziej urozmaicone sposoby. Stąd też jeśli otrzymasz podejrzaną wiadomość sugerującą zapłatę bądź kliknięcie w link na stronę której nie kojarzysz, skontaktuj się z usługodawcą. Wartym uwagi w przypadku otrzymania wiadomości mailowej sugerującej wykonanie określonej operacji, jest fakt iż należy sprawdzić czy adres mailowy dostawcy wiadomości jest poprawny.

[13] Źródło: Statista, https://www.statista.com/statistics/266155/number-of-phishing-domain-names-worldwide/ z dnia 01.07.2022 r.

Przykładowo otrzymany mail o finalizacji zakupu przedmiotu z serwisu OLX, powinien wyglądać dokładnie tak jak ten poniżej, jednakże nie na wszystkich urządzeniach nadawca ukazuje się automatycznie. Powyższe wynika ze specyficznej budowy aplikacji zainstalowanych na urządzeniach mobilnych, czego skutkiem jest wyświetlanie niepełnych informacji dotyczących nadawcy. Wskutek braku informacji o adresie mailowym, można w łatwy sposób paść ofiarą phishingu, którego następstwa mogą spowodować spore straty materialne, czy też utratę istotnych dla użytkownika danych wrażliwych.

Rys. 2 Prawidłowy mail OLX z widocznym nadawcą

Źródło: Materiał graficzny autorstwa własnego

Cyberprzestępcy wykorzystując fakt iż na wersjach mobilnych nadawca pozostaje ukryty podszywając się pod instytucję lub podmiot, może przygotować mail łudząco podobny do oryginalnego. Efektem tego na smartfonach lub tabletach otrzymać możemy mail dotyczący zakupu bez ukazanej informacji o fałszywym nadawcy. Określony mail wówczas może wyglądać jak poniżej.

Rys. 3 Mail phishingowy bez ukazanego nadawcy

Źródło: Materiał graficzny autorstwa własnego

Wiele osób, mało dociekliwych może paść w efekcie ofiarą cyberprzestepcy dokonując określonych w treści maila czynności. Aby upewnić się że mail nadawcy jest prawidłowy, na urządzeniu mobilnym należy kliknąć w “ptaszka” obok tekstu “do mnie”, wówczas ukazuje się nam cały adres mailowy nadawcy, co pozwala nam zidentyfikować czy jest On prawidłowy czy też fałszywy. Po wykonaniu powyższej instrukcji wyświetla nam się faktyczny adres nadawcy, który ukazuje kolejny rysunek.

Rys. 4 Mail phishingowy z widocznym nadawcą

Źródło: Materiał graficzny autorstwa własnego

Znając dotychczasowy e-mail nadawcy możemy skutecznie ustrzec się tym sposobem negatywnych skutków phishingu. Oczywiście zagrożeń cybernetycznych jak i tych stosowanych za pomocą socjotechniki jest znacznie więcej, dlatego warto regularnie przeprowadzać szkolenia i edukować się w zakresie protekcji przed nimi. Regularne zapoznawanie się z listą ostrzeżeń ogłaszanych na stronie internetowej CERT Polska zwiększyć może wiedzę w obszarze ochrony wrażliwych danych a także finansów. Ponadto skorzystać możemy z ogólnodostępnej rządowej Bazy wiedzy o cyberbezpieczeństwie na której również możemy uzyskać wiele informacji edukujących o zagrożeniach płynących z cyberprzestrzeni[14]. Pamiętajmy jednak że cyberprzestępcy nieustannie modyfikują metodykę ataków, zatem nie warto uzbroić się we wzmożoną czujność. Przestępczość transferująca do cyberprzestrzeni jest zjawiskiem z którym spotkał się niemal każdy obywatel Rzeczypospolitej Polskiej. Stosunkowo proste Modus operandi oraz wysublimowane techniki maskowania swoich działań są istotnym czynnikiem zwiększenia się zjawiska cyberprzestępczości w Polsce. Najpopularniejsze ataki skierowane w stronę obywateli, są określane mianem phishingu tj oszustwa komputerowego stanowiącego przestępstwo z art.287 § 1 oraz oszustwa internetowego, ściganego z art.286 § 1 kodeksu karnego. W perspektywie lat 2016 do pierwszego kwartału 2022 roku, ich łączna liczba wynosiła 282333 przypadki, z czego 214760 incydentów stanowiło przestępstwo oszustwa internetowego. Jak więc można zauważyć, ilość postępowań wszczętych przez organy Policji na terenie Rzeczpospolitej Polskiej ulegają zwiększeniu rok do roku. Skala zjawiska generuje konieczność skupienia uwagi na problematyce występowalności i wszczęcia działań o charakterze prewencyjnym jak i doraźnym, zmierzającym do redukcji przestępczości w Polskiej cyberprzestrzeni.

[14] Źródło: Strona Rządowa Rzeczypospolitej Polskiej, https://www.gov.pl/web/baza-wiedzy z dnia 17.10.2022 r.

1.3. Podmioty prawne odpowiedzialne za bezpieczeństwo cyberprzestrzeni w Polsce

Wiele krajów podjęło działania mające na celu walkę z przejawem cyberprzestępczości. Amerykanie utworzyli Departament ds. cyberprzestępczości, Unia Europejska utworzyła Europejskie Centrum ds. Walki z Cyberprzestępczością przy Europolu zaś w Polsce dnia 12 stycznia 2022 roku powołano Centralne Biuro Zwalczania Cyberprzestępczości. Powyższa jednostka utworzona została na mocy ustawy z dn. 17 grudnia 2021 roku, odpowiedzialna jest za eksplorację cyberprzestrzeni celem wykrywania cyberprzestępczości, rozpoznawania cech poszczególnych przestępstw i zwalczania.[15] Zwalczanie inteligentnego środowiska cyberprzestępczego nie jest łatwym zadaniem, zatem powyższe służby nie ograniczają się jedynie do swoich umiejętności i zasobów. Służby ds. zwalczania cyberprzestępczości aktywnie współpracują z Centralnym Biurem Śledczym Policji, Komendami Wojewódzkimi, a także organizacjami zajmującymi się monitorowaniem zjawisk przestępstw w cyberprzestrzeni. Wśród tych ostatnich należy wymienić należy Nask (Naukowa i Akademicka Sieć Komputerowa), będąca instytutem Państwowym powołanym w celu podjęcia badań nad rozwiązaniami, poprawy bezpieczeństwa i efektywności systemu rozwiązań teleinformatycznych.[16] W strukturach powyższej organizacji, funkcjonuje CERT Polska będący grupą powołaną do reagowania na wykryte incydenty w obszarze cyberprzestrzeni.[17] Czysto informacyjnie, warto aktualizować wiedzę zaś pod kątem cyberzagrożeń, o których informują powyższe informacje na swoich stronach internetowych.

Postępująca ewolucja w świecie cyfrowym, jako iż jej rozwój nastąpił w bardzo szybkim czasie, jest jednym z powodów dla których luki prawne pozwoliły przestępcom na przeniesienie się do świata wirtualnego. Jak donosi Naczelnik Wydziału do Walki z Cyberprzestępczością Komendy Wojewódzkiej Policji w Kielcach w wywiadzie problemem tak dużej ekspansji przestępstw w przestrzeni cybernetycznej jest eksterytorialna sprawczość przestępców na tym tle. Dokonywane określonego przedsięwzięcia komputerowego na terenie danego kraju w którym jest dozwolony, w innym kraju może być określany mianem przestępstwa w przypadku przeprowadzenia

[15] Źródło; Strona Rządowa, https://www.gov.pl/web/mswia/powstanie-centralne-biuro-zwalczania-cyberprzestepczosci z dnia 20.10.2022 r.
[16] Źródło; Nask, https://www.nask.pl/, z dnia 21.10.2022 r.
[17] Źródło; Cert, https://cert.pl/o-nas/ z dnia 21.10.2022 r.

cyfrowego nań ataku. Kolejnym problemem jest aspekt współpracy międzynarodowej krajów wschodniej granicy, krajami afrykańskimi lub azjatyckimi. Brak powzięcia kooperacji krajów wschodnich i afrykańskich w zatrzymanie przestępców, przyczynia się do eskalacji transferu przestępstw ze świata fizycznego do wirtualnego. Transgraniczność przestępstw, przyczyniła się do zwiększenia skali zjawiska, co przekłada się na większą ilość tworzony grup przestępczych w obszarze cybernetycznym.

Lata okresu pandemicznego, wywołanego przez eskalację rozprzestrzeniania się wirusa SARS-CoV-2 stanowiły zagrożenie na całym świecie, doprowadzając do skrajnego zmęczenia personele służb zdrowia. Tym samym, w wyniku restrykcji ustanowionych przez rządy w drodze legislacyjnej implementacji prawa, wiele osób zmuszonych było pozostać w domach w obawie przed utratą swego zdrowia fizycznego. Okres ten miał charakter izolacyjny, wobec którego wprowadzony zostały kwarantanny a także wdrożone prace w module hybrydowym czy też zdalnym. Firmy zatrudniające pracowników o powyższym charakterze pracy, miały możliwość dokonania redukcji kosztów stałych wynikających z doposażenia w miejscach pracy, tym samym pracownicy oszczędzali czas na dojazdy do pracy, co zwiększyło poziom wygody i ergonomii okresu samej pracy. Niefortunnie specyfika lat 2019-2022 stała się również idealnym środowiskiem dla cyberprzestępców. W wyniku prowadzenia polityki izolacyjnej w Rzeczpospolitej, Jak wynika z raportu badań "Polacy na e-zakupach z 2021 roku, sporządzonego przez Santander Consumer Bank, 35% Polaków, przed okresem szalejącej pandemii Covid-19 korzystała z mobilnej formy dokonywania e-zakupów. Rok później, ilość osób dokonujących owych zakupów internetowych wzrósł do 40%. W świetle przeprowadzonej ankiety, ciekawym jest fakt iż 80% ankietowanych, dokonało w 2020 roku zakupy przez internet. [18] Tak duży udział społeczeństwa Polskiego w realizacji zakupów za pośrednictwem internetu, stanowił oczywiste pole do zmiany modus operandi. Od drugiego kwartału 2020 roku, zatem od okresu światowo wprowadzanej pandemii odnotowane zostały wzmożone działania przestępców na rzecz zakładania domen phishingowych. Bowiem od tego okresu wzrost ilości zarejestrowanych domen mających za zadanie zmylić potencjalnego użytkownika sieci i tym samym dokonać kradzieży danych czy też środków finansowych wzrosła o

[18] Santander Consumer Bank, *Raport Polaków Portfel Własny, Polacy na e-zakupach,* 2021

około 384%[19] w stosunku do pierwszego kwartału 2020 roku. Tak drastyczny wzrost zmiany wektora działań przestępców, dokonało wzmożenia wystąpienia ataków o charakterze phishingowym. Wedle Krajobrazu bezpieczeństwa polskiego internetu, Raportu rocznego z działalności CERT Polska 2020 roku, ten zarejestrował aż 8310 oszustw komputerowych, w tym 7622 stanowiło ataki o charakterze phishingowym.[20] Ważnym jednak jest fakt iż powyższe dane są danymi wykrytymi przez CERT Polska, oraz zgłoszonymi przez użytkowników internetu. Skala zjawiska wydaje się jednak zdecydowanie większa. Wedle danych Komendy Głównej Policji, całkowita ilość wszczętych postępowań przeciwko zjawisku przestępstw komputerowych, wynosiła w roku 2020 aż 59781 wszczętych postępowań, zaś w roku 2021 liczba ta wzrosła aż do 83327 spraw. Dla porównania w roku 2016 liczba zgłoszonych przestępstw komputerowych wynosiła w Polsce 39860 wszczętych postępowań. Wynika bowiem z tego iż ewolucja społeczna, polegająca na jego ucyfrowieniu, przyczynia się do narastającego trendu wzrostu ilości przestępstw w Polsce. Skala zjawiska wskazuje iż w stosunku do roku 2016, przez pięć lat wzrosła ona ponad dwukrotnie[21]

1.4. Cyberterroryzm jako zagrożenie współczesnej cywilizacji

By poznać znaczenie pojęcia cyberterroryzmu, należy wgłębić się w jej fundamentalny termin i zdefiniować terroryzm. Jako iż pierwsze skojarzenia skłaniają nas ku pejoratywnych refleksji, należy dokładnie przeanalizować jego znaczenie. W języku łacińskim słowo “Terror” oznacza w ujęciu dosłownym strach bądź też grozę.[22] W ujęciu B. Hoffmana “terroryzm można uznać za przemoc lub groźbę przemocy, która zmierza do osiągnięcia celów politycznych lub służenia takim celom . Zgodnie z definicją zaproponowaną przez T. Hanuska „terroryzm jest to planowana, zorganizowana i zazwyczaj uzasadniona ideologicznie działalność osób lub grup mająca na celu wymuszenie od władz państwowych, społeczeństwa lub poszczególnych osób określonych świadczeń, zachowań lub postaw, a realizowana w przestępczych formach obliczonych na wywołanie szerokiego i maksymalnie zastraszonego rozgłosu w opinii

[19] Źródło; Statista, https://www.statista.com/statistics/266155/number-of-phishing-domain-names-worldwide/ z dnia 27.10.2022 r.
[20] NASK PIB/CERT Polska, *Krajobraz bezpieczeństwa polskiego internetu*, Raport roczny z działalności CERT Polska, Warszawa, 2020.
[21] Dane z Komendy Głównej Policji, z wykazu Krajowego Systemu Informacji Policji z zakresu lat 2016-2022,Warszawa z dnia 21.04.2022 r.
[22] Źródło: Wikipedia, https://pl.wikipedia.org/wiki/Terror z dnia 29.10.2022 r.

publicznej”[23]. Przyjąć zatem należy iż terroryzm co do zasady jest zjawiskiem użycia przemocy, będącej narzędziem do realizacji określonego celu. Terroryzm już od czasów starożytnych towarzyszył naszej cywilizacji, począwszy od Zelotów walczących o wyzwolenie Żydów spod ucisku politycznego Rzymian[24], przez Nizarytów, zwanych sykariuszami, mordujących znienawidzonych Seldżuków[25] aż po dzisiejsze odłamy ekstremistyczne np. Al-Ka’ida[26]. Terroryści w miarę upływu czasu, dokonują zmian w użyciu narzędzi służących do realizacji aktów terroryzmu. W Dobie postępu technologicznego i towarzyszącego w społeczeństwach środowiska cyfrowego, terroryści sięgają również po narzędzia umożliwiające dokonywanie ataków w cyberprzestrzeni. Należy zatem zdefiniować, czym jest tego typu zjawisko cyberterroryzmu w korelacji z klasyczną definicją terroryzmu.

Ewolucja klasycznego terroryzmu jest nieuchronnym procesem którego nie sposób zatrzymać. Nieodłącznym jednak elementem istoty bytu społeczeństw, jest byt ekstremicznych jednostek wyłamujących się spod zasad porządku publicznego. Owe jednostki wchodzące w posiadanie narzędzi mogące wywołać ogrom szkód na arenie międzynarodowej, istotnym jest zaznaczenie skali zagrożenia jakie działania terroru w cyberprzestrzeni mogą spowodować. W zamierzchłych czasach metodyka działań terrorystów zwanych Zelotami była stosunkowo prymitywna. Organizowane bunty i jednostek partyzanckich mających za cel destabilizację Cesarstwa Rzymskiego w wyniku ataków na strategiczne elementy zdawały się być początkiem ewolucji terroryzmu. W konsekwencji upływu wieków i przekazu z pokolenia na pokolenie idei Zelockiej, powstał ruch wspomnianych sykariuszy mordujących wybrane jednostki w miejscach wyjątkowo uczęszczanych. Dokonywano tego na potrzeby szerzenia na większą skalę trwogi, niepokoju i poczucia zagrożenia. W związku z dokonywaniem zbrojnej napaści w towarzystwie bezbronnych cywili, czy też atakowania składów magazynowych, zaimplementowali podwaliny pod obecnie występujący terroryzm.[27] Ten jednakże przechodzi pewną transformację bowiem zauważalnym jest wkraczanie

[23] I. Resztak, *НАУКОВИЙ ВІСНИК 4’ Львівського державного університету внутрішніх справ*, Львівського ,2011 s. 525.
[24] G. Chaliand, A. Blin, *Historia Terroryzmu, Od starożytności do Da'isz w przekładzie na j. Polski Katarzyny Pachniak,* [b.m.w.], 2020, s. 52.
[25] Źródło: Wikipedia, https://encyklopedia.pwn.pl/haslo/nizaryci;3947980.html z dnia 29.10.2022 r.
[26] Źródło: Wikipedia, https://pl.wikipedia.org/wiki/Al-Ka%E2%80%99ida z dnia 29.10.2022 r.

[27] *Ibidem,* G. Chaliand, A. Blin, *Historia Terroryzmu, Od starożytności do Da'isz w przekładzie na j. Polski Katarzyny Pachniak,* s. 54

przez organizacje ekstremistyczne w nowy odłam rzeczywistości, obszar cybernetyczny.

Cyberterroryzm zatem jest ucieleśnieniem definicji terroryzmu za użyciem narzędzi pozwalających na dokonywanie ataków w cyberprzestrzeni. Jako iż cyberprzestrzeń jest w procesie rozwoju technologicznego stosunkowo nowym tworem, a jej zasób opiewający w dane, infrastrukturę technologiczną a także możliwości jej użycia, stanowi istotny element terrorystycznego modus operandi wobec potencjalnych ofiar. Współczesny terroryzm oprócz stosowania konwencjonalnych metod zamierzchłych form jego stosowania, synchronizuje je również z przestępstwami w cyberprzestrzeni. Powyższe występuje za użyciem trzech obszarów mających zastosowanie zarówno w osobnej formie bytu, jak również w synchronizowanych metodykach działań, które to w połączeniu mogą wyrządzić szkody o niebagatelnych rozmiarach. Terroryści mając na uwadze postępujące zmiany w obszarze technologicznym, wykorzystują nowoczesne rozwiązania w trzech zasadniczych obszarach:

- Technologie informacyjne - jest wszechstronnym zestawem działań wykorzystujących środki technologiczne jak i oprogramowania, celem zastosowania ich w określonych obszarach w których łączy ze sobą zastosowanie obszarów pokrewnych takich jak informatyka, komunikacja oraz i środowisko komputerowe czy informacyjne)[28]
- Technologie teleinformatyczne - są szeregiem rozwiązań w postaci systemów czy też innych rozwiązań technologicznych pozwalających na automatyzację czy też dokonywanie czynności w środowisku cybernetycznym.[29]
- Technologie telekomunikacyjne - stanowi istotny człon przesyłu informacji z użyciem technologii pozwalającej na zdalne dokonywanie przekazu w formie cyfrowej, będącej elementem komputerowego buforowania, przechowywania i konwersji sygnałów na odległość[30]

[28] M. M. Sysło, *Technologia Informacyjna w edukacji*, [w:] *Poradnik dla nauczycieli informatyki w gimnazjum(18)*, Uniwersytet Wrocławski, [b.r.w.] s. 4
[29] K. B. Wydro, *Telematyka – znaczenia i definicje terminu*, [w:] *Telekomunikacja i techniki informacyjne 1-2/2005,* [b.m.w.], 2005, s. 116-117
[30] Źródło: Wikipedia, https://pl.wikipedia.org/wiki/Telekomunikacja z dnia 29.10.2022 r.

Ewolucja terroryzmu w cyberprzestrzeni przyczyniła się przejawów incydentów w wymienionych wyżej obszarach infrastruktury technologicznej. Mimo iż przejawami działań środowisk ekstremistycznych są z reguły motywy na tle wyzwoleńczo-ideowym, religijnym lub polityczno-gospodarczym, warto zaznaczyć iż powyższe przejawiać się może za użyciem infrastruktury technologicznej. Sektor ten bowiem ma w posiadaniu ogrom danych, informacji, teleinformacji oraz sygnałów pozwalających na zamierzone wykorzystanie przez wyspecjalizowanego ekstremistę. W dobie XX-wieku cyberterroryzm dokonywany jest formie podobnej do znanych nam klasycznych zjawisk ataków grup ekstremistycznych. Realizowany jest on bowiem za użyciem środków, pozwalających na ingerencję w infrastrukturę technologiczną, celem wywołania określonych celów. Należeć do nich mogą na przykład:[31]

- Wywołanie określonego procederu technologicznego (np. uruchomienie głowicy bomby nuklearnej czy też unieruchomienie systemu obronnego danego państwa)
- Utrudnienie w dostawie lub przerwania usług (np. Zakłócanie sygnałów bądź uniemożliwienie działania poszczególnej infrastruktury)
- Przechwycanie kluczowych informacji (np. na potrzeby planowania kolejnych ataków terrorystycznych)
- Manewrowe przesyły fałszywych informacji (przeprowadzane ku strategicznemu zmyleniu grup antyterrorystycznych) Ideologiczne przeprowadzanie propagandy (Szerzenie informacji o ustalonym charakterze w danej społeczności)

Jak zatem można zauważyć, powyższe obszary działania jednostek cyberterrorystycznych mogą spowodować powstanie zagrożenia w sektorach które wykorzystują nowoczesne systemy teleinformatyczne do swego funkcjonowania. Zjawisko terroryzmu, tudzież omawianego cyberterroryzmu charakteryzuje się nagłym jego wystąpieniem, zatem istotnym jest aktualizacja procedur bezpieczeństwa oraz wprowadzanie nieustannych zmian w systemach bezpieczeństwa danych sektorów.

[31]R. Kołodziejczyk, *Nowa Odsłona Terroryzmu – Cyberterroryzm*, Wydział Prawa, Administracji i Zarządzania Uniwersytetu Jana Kochanowskiego, Kielce,, s. 148

1.5. Cyberbezpieczeństwo Rzeczypospolitej Polskiej w ujęciu technologicznym

Nieustanna implementacja zabezpieczeń w obszarze cyberprzestrzeni jest kluczowym do stworzenia bezpiecznych warunków funkcjonowania zarówno społeczeństwa w nim operującego, firm a także Państwa. Biorąc pod uwagę znaczenia istoty jak i charakteru tworu jakim jest Państwo, winno się przypomnieć zamierzenie jego utworzenia.

Jak czytamy w art. 5 Konstytucji Rzeczypospolitej Polskiej, "Rzeczpospolita Polska strzeże niepodległości i nienaruszalności swojego terytorium, zapewnia wolności i prawa człowieka i obywatela oraz bezpieczeństwo obywateli, strzeże dziedzictwa narodowego oraz zapewnia ochronę środowiska, kierując się zasadą zrównoważonego rozwoju."[32] Istotnym zatem jest podjęcie działań sprostających wymaganiom zmieniającego się technologicznie świata. Zabezpieczenie obszaru cyberprzestrzeni Polski jest zatem nie możliwością, a obowiązkiem wynikającym z zapisów konstytucyjnych w wymiarze ogólnym jej funkcjonowania w dzisiejszym świecie. Ochrona środowiska cybernetycznego jest istotą podjętej strategii mającej na celu podniesienie bezpieczeństwa na terenie kraju.
Do jej skutecznej realizacji, podjęto utworzenie w 2013 roku Polityki Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej. Mając na uwadze nieustanny rozwój cyfryzacji w skali światowej, podjęte zostały strategiczne działania w obszarze bezpieczeństwa Państwa Polskiego w cyberprzestrzeni. Głównym ich celem jest osiągnięcie poziomu bezpieczeństwa uznanego za akceptowalny w dalszym funkcjonowaniu kraju nad Wisłą. Do realizacji zadań w powyższym obszarze wyznaczone zostały określone poniższe cele szczegółowe działań:[33]

– Realizacja działań mających na celu poprawę poziomu bezpieczeństwa infrastruktury teleinformatycznej Polski.
– Dokonywanie zwiększenia potencjału obronnego, pozwalającego na zapobieganie a także zwalczanie incydentów stwarzających zagrożenie w cyberprzestrzeni.

[32] Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. 1997 nr 78 poz. 483)

[33] Rzeczpospolita Polska, Ministerstwo Administracji i Cyfryzacji, Agencja Bezpieczeństwa Wewnętrznego, *Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej*, Warszawa, 25 Czerwca 2013 r.

– Redukcję zjawisk mogących przyczynić się do zmniejszenia poziomu bezpieczeństwa teleinformatycznego.
– Wyznaczenie określonych struktur podmiotów realizujących kompetencje w zakresie bezpieczeństwa Państwa w cyberprzestrzeni.
– Dokonanie utworzenia rządowego systemu zarządzania w ramach struktur państwowych w obszarze bezpieczeństwa cybernetycznego, wraz z utworzeniem zakresu wytycznych dla podmiotów niepublicznych.
– Opracowanie trwałego systemu koordynacji i wymiany informacji przez wyznaczone podmioty uprawnione do ochrony cyberprzestrzeni i jej użytkowników na terenie Rzeczypospolitej Polskiej
– Realizacja podniesienia świadomości w obszarze zagrożeń, metodyki działań a także środków bezpieczeństwa w cyberprzestrzeni.

Bezpieczeństwo struktur funkcjonowania Państwa jest priorytetowym przedmiotem pracy instytucji, służb i organów administracji zarówno zespolonej jak i niezespolonej. Z racji nadrzędnej istoty konieczności zapewnienia bezpieczeństwa na każdym szczeblu, powołana do życia została Ustawa o Krajowym Systemie Cyberbezpieczeństwa dnia 1 sierpnia 2018 roku. Powyższa ustawa została wprowadzona przez Prezydenta Rzeczypospolitej Polskiej w ramach wdrożenia w drodze legislacyjnej Dyrektywy Parlamentu Europejskiego i Rady Unii Europejskiej w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii.[34] Implementacja powyższej ustawy miała znacząco wpłynąć na bezpieczeństwo Państwa Polskiego w obszarze cyberprzestrzeni. Powyższy system jest kluczowym rozwiązaniem protekcyjnym zapewniającym bezpieczeństwo cyberprzestrzeni w obszarze istotnych usług kluczowych stanowiących instytucje i firmy o charakterze krytycznym, a także usług cyfrowych na terenie Polski. Ponadto jego implementacja na szczeblach administracyjnych stanowi podwaliny pod stworzenie warunków wysokiej jakości bezpieczeństwa systemów teleinformatycznych w powyższych obszarach. W szczególności ustawa ta definiuje sposób organizacji krajowego systemu cyberbezpieczeństwa wraz z ustaleniem zakresu zadań poszczególnych podmiotów wchodzących w skład owego systemu, sposób dokonywania nadzoru i kontroli a także

[34] Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. 1997 nr 78 poz. 483)

strategię do zachowania najwyższego poziomu bezpieczeństwa. Powzięte procedury legislacyjne mające stworzyć okoliczności prawne umożliwiające na dokonanie zmiany przestrzeni cyfrowej, wymagają jednak obsługi podmiotów zobligowanych do wykonywania ściśle określonych kompetencji w omawianym obszarze działań. Podmiotami objętymi jej regulacjami objęte są poniższe podmioty ujęte w art. 4, ust. 1-20 ustawy o krajowym systemie cyberbezpieczeństwa z dnia 5 lipca 2018 r. Wyszczególnione we wspomnianej ustawie jednostki, zobligowane są do współdziałania i realizowania zadań mających na celu podniesienie poziomu bezpieczeństwa i odporności na zagrożenia występujące w obszarze cyberbezpieczeństwa. W ramach strategii, wyszczególnionych zostało pięć kluczowych celów których realizacja ma poprawić potencjał obronny Rzeczypospolitej w omawianej sferze. Pięć celów nadrzędnych o których mowa obejmują działania na rzecz:[35]

1. Nieustannego podnoszenia jakości i poziomu Krajowego Systemu Cyberbezpieczeństwa;
2. Podniesienia możliwości operacyjnych pozwalających na zwiększenie odporności systemów informacyjnych zarówno administracji publicznej jak i sektora prywatnego. Ponadto istotnym jest spełnienie poziomu obronnego w zakresie skutecznego zapobiegania i reagowania na incydenty poprzez narodowe standardy w obszarze cyberbezpieczeństwa;
3. Wsparcia sektora cyberbezpieczeństwa oraz zwiększenie jego potencjału na terenie Rzeczypospolitej Polskiej;
4. Uświadamiania społeczeństwa w obszarze cyberbezpieczeństwa wraz z podwyższeniem ich kompetencji ku niemu;
5. Budowy silnej pozycji na arenie międzynarodowej w ujęciu cyberbezpieczeństwa.

Powyższe cele określone zostały celem kompleksowego zapewnienia ochrony w przestrzeni cyfrowej na terenie Polski. Istotą realizacji powyższych ramowych działań, jest fundamentalnym obszarem budowania wysokiej odporności na zagrożenia mogące zaburzyć prawidłowe funkcjonowanie Państwa. Poszczególne cele oraz propozycje rozwiązań zawarte w ustawie, stanowią jednolity zbiór kompetencji, mający dokonać ochrony najważniejszych struktur i infrastruktur Państwowych, z bezpieczeństwa

[35] *Ibidem*

społeczeństwa w cyberprzestrzeni. W ramach realizacji obszarów, przewidywane jest wsparcie skuteczności działań organów ścigania a także wymiaru sprawiedliwości w afroncie do zagrożeń szpiegostwa czy też terroryzmu w cyberprzestrzeni, przy uwzględnieniu operacyjności Sił Zbrojnych Rzeczypospolitej Polskiej.[36]

Cyberprzestrzeń w ujęciu charakterystyki zagrożeń, nie różni się zbytnio od fizycznego wymiaru bezpieczeństwa krajowego. Jako iż Państwo jest zagrożone ze wszechstron, czy to poprzez próby szpiegostwa służb wywiadowczych innych państw, czy też w obszarze widma incydentów terrorystycznych. To jednak nie wszystkie zagrożenia z jakimi Państwo Polskie liczy się realizując swe zadania obronne w obszarze cyberprzestrzeni. Najczęstszymi typami zagrożeń występujących w cyberprzestrzeni Polskiej, są[37]:

– Ataki wykorzystujące socjotechnikę do wyłudzenia danych;
– Utratę tożsamości powszechną w dobie zmasowanych ataków phishingowych, vishingowych czy smishingowych;
– Kradzież danych i ich sprzedaż na Darknecie, a także towarzyszący jej często stosowany proceder warunkowego okupu pod groźbą zniszczenia owych danych;
– Zagrożenia dostępu do poszczególnych usług w wyniku ataku polegającego na zakłóceniu możliwości skorzystania z usługi (DoS) bądź też poprzez rozproszoną jego wersję (DDoS);
– Ataki z użyciem oprogramowania mającego dokonać szkód w sprzęcie komputerowym;
– Ataki niechcianymi e-mailami mogących doprowadzić do zawieszenia się serwerów;

W celu skutecznej realizacji programu ochrony cyberprzestrzeni przez podmioty krajowe do tego uprawnione, nadrzędnym uwarunkowaniem jest jednak ujednolicenie definicji cyberprzestrzeni. Co prawda niemal niewykonalnym jest ugruntowanie poszczególnych definicji składowych sfery cyfrowej, jednakże na terenie Unii Europejskiej w ramach wspólnoty Europejskiej, państwa członkowskie winne są podjąć

[36] Ministerstwo Cyfryzacji, *Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022*, Warszawa, 2017, s. 6
[37] M. Grzelak, K. Liedel, *Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski – zarys problemu*, [b.m.r] s. 131

politykę wdrożenia jednolitego prawa w omawianym obszarze. Powyższe jest o tyle niezbędnym, że stanowi podstawę do jednowymiarowego traktowania zjawiska cyberprzestępczości i podejmowanie szybszej i co najważniejsze skuteczniejszej koordynacji a także metod obrony przed incydentami w przestrzeni cybernetycznej. Problematyka ta jest ówcześnie przedmiotem wielu nieścisłości w podejmowaniu czynności śledczych czy też interwencyjnych, co uniemożliwia skuteczniejsze dokonywanie działań na rzecz zapewnienia bezpieczeństwa w cyberprzestrzeni.[38]

Incydenty stosowania ataków na poszczególne sektory państwowe są szczególnie niebezpieczne. Ich występowalność jest bowiem dość duża. W Polskiej cyberprzestrzeni w samym roku 2021 CSIRT NASK zaklasyfikował 36 zagrożeń jako istotnie poważne. Stanowiło to zagrożenie w usługach kluczowych które mogły doprowadzić do niekorzystnego dla Bezpieczeństwa Polski zakłócenia niektórych usług. Wśród nich, 31 stanowiło incydenty dotyczące sektora bankowego 3 zaś dokonane zostały w sektorze energetycznym zaś 2 w sektorze ochrony zdrowia. Wśród podmiotów administracji Państwowej, całkowita ilość zarejestrowanych zagrożeń opiewała w liczbie 512 incydentów. Wedle raportu CERT NASK, kolejnym istotnym zagrożeniem było również wykrycie oprogramowania Flubot o zdolności do błyskawicznego rozproszenia się z użyciem środka przesyłu SMS. Całkowita ilość zarejestrowanych incydentów wyniosła finalnie w 2021 roku 23308 zagrożeń, z czego ponad połowa z nich opisana była na liście ostrzeżeń[39]. O szczegółowym zjawisku dokonywania ataków na poszczególne sektory Państwa dowiedzieć się możemy z tabeli incydentów obsłużonych przez CERT Polska w 2021 r. w podziale na sektor gospodarki.[40] Oto jedne z największych incydentów:

– WannaCry - jest oprogramowaniem typu ransomware mającym na celu przeprowadzenie ataku na jednostki komputerowe i dokonania okupu w zamian za uzyskanie oprogramowania deszyfrującego, pozwalającego na odblokowanie dostępu do urządzeń. WannaCry jest wirusem który w sposób spektakularny zainfekował ponad 300 tysięcy komputerów w 99 krajach świata, w tym komputery ministerstwa spraw wewnętrznych Rosji.[41]

[38] *Ibidem, s. 137*
[39] Raport roczny z działalności CERT Polska, *Krajobraz bezpieczeństwa polskiego internetu 2021,* s. 21
[40] *Ibidem, s 22-24*
[41] Źródło: Wikipedia, https://pl.wikipedia.org/wiki/WannaCry z dnia 29.11.2022 r.

– TitanRain - jest kolejnym spektakularnym zestawem ataków, przeprowadzonych w kierunku sprzętów komputerowych USA w formie wirusów. Jak zaznacza Rząd USA, przeprowadzone ataki zostały przez Chińską Armię Ludowo-Wyzwoleńczą. Na przestrzeni trzech lat skoordynowane zostały ataki, wykradające dane szeregu kluczowych podmiotów o znaczeniu państwowym takich jak m.in. NASA czy FBI. [42]

– Operacja Malezja - jest dość niezwykłym przejawem stronniczości grupy hakerów z całego świata, mianujących się jako Anonymous. Rząd Malezji dokonał bowiem blokady dostępu do stron internetowych Wikileaks - czyli strony na której możemy dokonać zamieszczenia w sposób anonimowy informacji, oraz strony The Pirate Bay będącej stroną do przesyłania plików. W odpowiedzi na poczynania rządu, dokonano skoordynowanego ataku na 91 stron, celem zadeklarowania solidarności ze społeczeństwem i jego podstawowym prawem dostępu do informacji.[43]

[42] Źródło: Wikipedia, https://en.wikipedia.org/wiki/Titan_Rain z dnia 29.10.2022 r.
[43] Źródło: Wikipedia, en.wikipedia.org/wiki/Timeline_of_events_associated_with_Anonymous z dnia 29.10.2022 r.

Rozdział 2. CYBERPRZESTĘPCZOŚĆ W ASPEKCIE BADAWCZYM

Ujmując zjawisko cyberprzestępczości w kategorii rozważań naukowych, priorytetowym przedmiotem badań jest szczególnie tematyka bezpieczeństwa. Mając na uwagę eskalację zjawiska, podejmowane są bowiem analizy potencjalnych zagrożeń w ujęciu zarówno jednostkowym, jak i o charakterze państwowym tudzież nawet regionalnym.[44] Jako niepodważalny element skutecznego gospodarowania Państwa, bezpieczeństwo oraz metodyka działań prewencyjnych, zmierzających do ograniczenia występowalności zagrożeń, stanowi priorytet działań. Kolejnym obiektem rozważań środowiska naukowego jest cyberprzestępczość. Stała się ona również sektorem zainteresowania środowiska prawniczego. Problematyka cyberprzestępczości stanowi bowiem realne zagrożenie dla wszystkich grup społecznych, organizacji, podmiotów prawnych a także rządów danych państw. W związku z powyższym na tle naukowym, rozważane są możliwości implementacyjne zmian prawnych, które to w procesie legislacyjnym przyczynić się mogą do poprawy kooperacji służb Państw na arenie międzynarodowej. [45]

2.1. Cyberprzestępczość – priorytetowy przedmiot badań

Eskalacja zjawiska cyberprzestępczości przez inteligentne środowiska operujące w świecie teleinformatycznym sprawia iż potencjalnie bezpieczeństwo każdego obywatela a także instytucji może być potencjalnie podatne na atak. W obliczu coraz większego zagrożenia na tle cybernetycznym, zasadnym wydaje się być stwierdzenie iż należy podjąć wzmożona mobilizację w kierunku zwalczania cyberprzestępczości. Decyzja Rządu Rzeczypospolitej o powołaniu Centralnego Biura Zwalczania Cyberprzestępczości w styczniu 2022 roku, świadczy o konieczności zapobiegania dalszej dynamiki wzrostu zjawiska. Poniższa praca badawcza ma na celu ukazanie charakterystyki zjawiska a także zastosowanie metodyki przeciwdziałania atakom na społeczeństwo. Określenie czynników będących asumptem do działania dla

[44] Źródło: J. Kosiński, *Paradygmaty cyberprzestępczości - Wstęp*, 2015, s. 10, (https://depot.ceon.pl/bitstream/handle/123456789/7280/Paradygmaty-cyberprzestepczosci-wstep.pdf?sequence=4&isAllowed=y)
z dnia 27.10.2022 r.
[45] J.Wasilewski, *Cyberprzestępczość - Wybrane Aspekty Prawnokarne I Kryminalistyczne*, Uniwersytet W Białymstoku Wydział Prawa, Białystok, 2017, s. 5.

cyberprzestępców, analiza najczęstszych podatności oraz warunków środowiska teleinformatycznego a w szczególności metodyki zapobiegania incydentom są kluczowe dla zrozumienia zjawiska. Mając na uwadze już występujące ataki w cyberprzestrzeni, trendy i problematykę środowiska wyciągnąć można konkluzje dzięki którym wskazać można pożądane zakresy działań, celem redukcji występowalności przestępstw o charakterze cybernetycznym. W oparciu o powyższe czynniki oraz wiedzę w zakresie zapewnienia ochrony przed atakami, poprzez gruntowną analizę i wyciągnięcie stosownych doświadczalnych wniosków, możemy zaimplementować działania skutkujące redukcją podatności na atak cybernetyczny. Najważniejszym elementem eksploracji obszaru niniejszych badań zjawiska przestępczości w cyberświecie jest redukcja podatności na atak w społeczności Rzeczypospolitej Polskiej. Mając na uwadze wzrost ilości osób poszkodowanych, poruszone rozważania będą miały charakter promocji działań protekcyjnych. Świadomość istnienia narzędzi, procedur i technik pozwalających efektywnie zarządzać podatnościami na ataki, monitorowania bezpieczeństwa a także jego zwalczania jest istotą cybersecurity managementu. Najważniejszymi aspektami w ujęciu *sensu largo* cyberprzestępczości jest nadanie wartości szeroko pojętej treści, by sens jej przekazu mógł przedstawić nowy rodzaj postrzegania zagrożeń ze strony cyberbezpieczeństwa, zarówno społeczeństwu jak i środowisku badawczemu. Rozważania nad paradygmatem cyberprzestępczości w aspekcie eskalacji zagrożeń jest o tyle istotnym tematem co skala jego występowalności. Zastosowanie ogólnej metodologii w opisywanym opracowaniu w zderzeniu z metodologią opisową i normatywną pozwala na ekstrapolację założeń które mogą być skutecznie stosowane w wielu przedsiębiorstwach, instytucjach ale i przez osoby fizyczne.

2.2. Etiologia zjawiska cyberprzestępczości

Powszechna cyfryzacja, i pole do eksploracji przez przestępców zasobów informatycznych, transgranicznym udziale w dokonywanym przestępstwie zdaje się być niewymagającym a co za tym idzie bezpieczniejszym sposobem na dokonywanie przestępstw. Kompilacja dotychczasowych założeń prawnych wynikająca z trendu cyfryzacji zjawiska dostępności internetowej do bankowości elektronicznej, elektronicznych dokumentów a także do szerokiego spektrum informacji i możliwości zarządzania nimi jest bardzo pożądaną okolicznością dla przestępców. Zagrożenie

omawiane powyżej, jest obszarem badań ekspertów z całego świata. Eskalacja zjawiska możliwa jest dzięki charakterystyce środowiska cyfrowego cechowanego przez:

- Transgraniczność - sprawni cyberprzestępcy mają możliwość dokonywania przestępstwa z dowolnego miejsca na ziemi dzięki łączności teleinformatycznej z wykorzystaniem komputera. Zwiększa się tym samym zasięg działania sprawcy i możliwość zdalnego zaatakowania potencjalnej ofiary;
- Anonimowość - ukrycie swojej tożsamości oraz miejsca przebywania ze względu na rozwiązania technologiczne typu sieć VPN, umożliwia na dokonanie przestępstwa, maskując swoje położenie, posługując się IP randomowego użytkownika sprzętu komputerowego. Właśnie między innymi dlatego zidentyfikowanie przestępcy poprzez intensywne poszukiwania śladów cyfrowych staje się znacznie utrudnione zarówno przez sam proces, jak i różnice w jurysdykcjach powiązanych krajów w obszarze penalizacji tychże przestępców;
- Ogólnodostępność - By dokonać cyberprzestępstwa, potrzebne jest jedynie urządzenie komputerowe oraz połączenie z siecią internetową. Przestępca mający wiedzę w obrębie struktury budowy systemów teleinformatycznych, chcący dokonać ataku, może go zrealizować zarówno w bibliotece, w galerii handlowej a także znad plaży na Bahamach;
- Niematerialny charakter - wszystkie zapisy i informacje w sieci, mają charakter cyfrowy, co oznacza iż wszelkie zapisy znajdują się w cyberprzestrzeni, nie fizycznie. Zdobycie takowych informacji przez sprawnego hakera może być powielone na setkach nośnikach a także w sieci;
- Brak określonego centrum kontroli cyberprzestrzeni - Różnice w jurysdykcji poszczególnych państw, sprawiają iż przestępstwa na tle międzynarodowym, są trudne do wyegzekwowania prawnego. Mimo iż poszczególne kraje mogą mieć wyspecjalizowane Państwowe Biura ds. walki z cyberprzestępczością, różnice w kazusach prawnych sprawiają że penalizowane danego czynu bywa rozbieżne.

Wkroczenie światka przestępczego w cybernetyczną strefę środowiska, okazało się być preludium do intensyfikacji popełnianych przestępstw. Dzięki możliwości dokonywania ataku na obrany cel z dowolnego miejsca na ziemi, przy jednoczesnym tuszowaniu adresu IP poprzez przekierowywanie go na inne regiony geograficzne,

Hakerzy są w stanie dokonać przestępstw uniemożliwiając lub znacząco utrudniając wykrycie przez organy ścigania. Gama zasobów danych możliwych do hakowania, kradzieży czy zniszczenia jest ogromna. Szacuje się iż w 2022 roku świat powinien wytworzyć w okolicach 94 zetabajtów czyli 94 tryliona bajtów[46]. Liczba ta wydaje się być astronomiczną i wraz z postępem technologicznym oraz coraz większą liczbą połączonych ze sobą używanych urządzeń, liczba ta będzie systematycznie wzrastać. Tak ogromny zasób danych to święty Graal dla wyedukowanych cyberprzestępców. Nieustannie powiększające się pole zasobów możliwych do przejęcia, wraz z możliwościami maskowania swojego położenia za pomocą użycia sieci VPN (wirtualna sieć prywatna) sprawia iż taki stan rzeczy staje się być zachętą do ułatwionego przestępczego działania. Zjawisko cyberprzestępczości znane jest od czasów powstania technologii komputerowej. W dobie rozwoju technologicznego oraz coraz bardziej zróżnicowanych form ataku, przy jednocześnie korzystnej infrastrukturze w świecie cybernetycznym, doprowadza do eskalacji zagrożeń związanych z przestępczością w sieci. Teleinformatyka w Polsce, w wymiarze dostępu do internetu na dobre zagościła dopiero w 1993 roku. Materiał "Obywatele Internetu" ukazany na potrzeby konferencji odbytej w Trzebinie w 29.06.1999 roku wskazuje iż liczba polskich użytkowników internetu stanowiła ponad milion obywateli. Jak wskazuje raport Bezpieczni na e-zakupach 2022, przeprowadzone badania przez Santander Consumer Bank dają wynik 87% korzystających z internetu osób w Polsce.[47] Tak wysoki wskaźnik sugeruje iż należy gruntownie przebadać obszar środowiska teleinformatycznego, celem redukcji zjawiska cyberprzestępczości w Polsce. Mając na uwadze środowisko przestępcze w cyberprzestrzeni, zauważyć możemy iż w perspektywie lat 2016-2022, trend przestępczości w rośnie z roku na rok coraz bardziej. Wykaz owej eskalacji obrazuje nam poniższa tabela:

Tabela 1. Tabela postępowań wszczętych o charakterze cyberprzestępstw w latach 2016-2022

	Liczba wszczętych postępowań według poszczególnych lat						
	2016	2017	2018	2019	2020	2021	2022[48]

[46] Źródło: Financesonline, https://financesonline.com/how-much-data-is-created-every-day/ z dnia 22.10.2022 r.
[47] Santander Consumer Bank, *Raport Polaków Portfel Własny Bezpieczni na e-zakupach,* 2022.
[48] Przedstawione statystyki Policji dotyczą łącznej ilości wszczętych postępowań odnotowanych do pierwszego kwartału 2022 roku.

Art. 286 § 1 Oszustwo Internetowe	26901	28759	29921	32161	35031	48884	13103
Art. 287 § 1 Oszustwo Komputerowe	4057	4508	7344	10714	11132	21119	8699

Źródło: Opracowanie własne w oparciu o dane z Komendy Głównej Policji, z wykazu Krajowego Systemu Informacji Policji z zakresu lat 2016-2022, Warszawa z dnia 21.04.2022 r.

Analizując powyższe, dojść można do wniosku iż wzrost cyberprzestępczości w oparciu o dane ze wszczętych postępowań Policji wskazuje iż ich eskalacja z roku 2017 wynosiła 6.34% większą występowalność w stosunku do roku 2016. Kolejny rok ukazuje nam już trend na poziomie 11.59% wzrostu wszczętych postępowań w zakresie przestępstw komputerowych. W roku 2019, tuż przed kryzysem pandemicznym, wskazywał iż współczynnik wzrostu cyberprzestępczości w Polsce podniósł się o 20.67% w stosunku do roku poprzedniego. Chociaż w 2020 roku cyberprzestępczość wydawała się przyhamować, to nieznaczny wzrost o 4,74% wskaźnika nadal stanowił trend eskalacyjny. Przełomem jednak okazał się być rok 2021, w którym to zarejestrowano spektakularny bo 39.39% wzrost ilości wszczętych postępowań przeciwko przestępczości zorganizowanej. Przypuszczać możemy zatem iż okres pandemicznej izolacji, zamknięcia się w pomieszczeniach skutkować mogło zwiększoną aktywnością użytkowników w internecie. W porównaniu do omawianych wcześniej trendów rejestracji domen phishingowych, wydawać by się mogło iż cyberprzestępcy celowo wzmożyli swoją aktywność w okresie pandemii, z uwagi na zwiększone możliwości korzystania z infrastruktury cybernetycznej a także zjawiska społecznego wzrostu użytkowania sieci. Zastanawiającym jest jednak rok 2022 który to już w pierwszym kwartale odnotował 25573 przypadków wszczęcia postępowań z tytułu przestępstw komputerowych co stanowi w przybliżeniu 30,7% ze wszystkich postępowań z roku 2021-go. Zakładając iż trend nadal będzie zmierzał ku wzrostowi a dotychczasowe przestępstwa cybernetyczne będą miały charakter nieustępliwy, założyć można iż w 2022 roku liczba wszczętych postępowań może oscylować w granicy 102292 przypadków zgłoszonych, wobec których podjęte zostaną działania przez Policję. Stanowić to może 22.76% kolejnego wzrostu omawianych ilości przestępstw w Polsce. Tak duża skala zjawiska jest przykładem na to że należy gruntownie zacząć działać zarówno w formie prewencyjnej, jak i doraźnej, podnosząc świadomość społeczeństwa w obszarze cybernetycznym, a także zmierzając ku ujednolicenia prawa

na tle międzynarodowym, by umożliwić kooperację służb celem wykrycia cyberprzestępców.[49] Ogrom i różnorakość dokonywanych przestępstw na tle cybernetycznym jest porażająca. Zjawisko ewoluując, ukazało szereg typologii działań o znamionach określanych jako cyberprzestępstwa. Ich typizacja pozwoliła na dopasowanie znamion przestępstwa dokonanego przy użyciu sprzętu komputerowego na określone kategorie i podkategorie. Mimo iż definicja przestępstw popełnianych za pośrednictwem urządzenia komputerowego była wyjątkowo trudna ze względu na identyfikację i rozbieżności w zastosowaniu poszczególnych kazusów prawnych do typów przestępstw. *U*stanowienie Konwencji ETS 185 stało się *De lege lata*[50] podwaliną do możliwości kategoryzacji cyberprzestępstw wedle ich charakteru. Konwencja ta stanowiła jednolity traktat międzynarodowy poprzez standaryzację przepisów prawnych na terenie Państw członkowskich Rady Europy oraz Państw Sygnatariuszy takich jak Stany zjednoczone, Kanada, RPA oraz Japonia. Określenie wspólnej interkontynentalnej polityki ds. bezpieczeństwa w cyberprzestrzeni, tworzonej przez ekspertów, stało się kanwą międzynarodowego prawa penalizującego w obszarze cybernetycznym.

Określone podstawy do identyfikacji przestępstw dokonywanych w cyfrowym środowisku weszły w życie w 45 z 53 państw będących stronami Konwencji. Stały się one prekursorskim asumptem do międzynarodowej współpracy w karno-procesowym aspekcie zwalczania cyberprzestępstw[51]. Istotnym elementem dołączenia tak wielu Państw do powyższej Konwencji, zdecydowanie stał się fakt iż cyfrowe środowisko, stworzyło przestępcom możliwości do przeprowadzenia opłakanych w skutkach ataków na infrastrukturę teleinformatyczną. Narażona również została infrastruktura krytyczna która będąc kluczowym elementem polityki bezpieczeństwa Państwa, nie mogła dopuścić do takowych zagrożeń. Securyzacja oraz wdrożenie międzynarodowej legislacji koordynującej działania i zakres współpracy Państw objętych Konwencją znacznie ułatwia podejmowanie penalizacji przestępstw dokonanych w cyberprzestrzeni. Mimo iż kraje wschodnie oraz wschodnioazjatyckie nadal mają rozbieżności jurysdykcyjne wobec cyfrowych przestępców, to jednak współpraca

[49] Wyliczenia na podstawie danych z Komendy Głównej Policji, z wykazu Krajowego Systemu Informacji Policji z zakresu lat 2016-2022, Warszawa z dnia 21.04.2022 r.

[50] Z języka łac. "Z Punktu Widzenia Prawa".

[51] I. A. Jaroszewska, *KPP Monografie Wybrane aspekty przestępczości w cyberprzestrzeni Studium prawnokarne i kryminologiczne,* Olsztyn, 2017, s. 9.

między krajami zachodnimi, połączonymi ów Konwencją, jest znacznie bardziej uregulowania legislacyjnie. Typizacja cyberprzestępstw wedle wyżej wymienionej Konwencji określiła pięć poniższych docelowych segmentów ataków które zwalczane zostać mają wedle uznanych za niezbędne w danym kraju środków prawnych. Segment pierwszy przestępstw przeciwko poufności, integralności i dostępności danych informatycznych i systemów ukazuje poniżej opisana tabela.

Tabela 2. Tabela przestępstw przeciwko poufności, integralności i dostępności danych informatycznych i systemów

– Nielegalny dostęp - charakteryzujący się umyślnym i bezprawnym uzyskaniem dostępu do całości lub części infrastruktury systemu informatycznego z zamiarem naruszenia zabezpieczeń i pozyskania określonych danych informatycznych. Przestępstwo też uznawane jest w odniesieniu do systemu informatycznego który połączony jest z innym systemem informatycznym – Nielegalne przechwytywanie danych - W ujęciu Konwencji jest to umyślne i bezprawne przechwytywanie z użyciem urządzeń technicznych, niepublicznych transmisji danych informatycznych do, z, lub w ramach systemu informatycznego włącznie z emisjami elektromagnetycznymi – Naruszenie integralności danych - charakteryzuje się bezprawnym dokonywaniem niszczenia, wykasowywania, uszkadzania, dokonywania zmian lub usuwania danych informatycznych. – Naruszenie integralności systemu - będące umyślnym, bezprawnym, poważnym w skutkach zakłócaniem funkcjonowania systemu informatycznego poprzeez jakkolwiek wprowadzenie, transmisję, zniszczenie, wykasowywanie, uszkadzanie czy dokonywanie zmian lub usuwanie danych informatycznych – Niewłaściwe użycie urządzeń - ten typ przestępstwa charakteryzuje się umyślnym a także bezprawnym zakłócaniem prosperowania systemu informatycznego poprzez dokonywanie wprowadzenia, transmisji, niszczenia, wykasowania, uszkadzania, dokonywania zmian lub usuwania danych informatycznych.

Źródło: Konwencja Rady Europy o cyberprzestępczości, z dnia 23 listopada 2001 r. Budapeszt, Art. 2-6 www.prawo.pl/akty/dz-u-2015-728,18197508.html z dnia 20.08.2022 r.

Segment drugi określa zaś tabela przestępstw komputerowych.

Tabela 3. Tabela przestępstw komputerowych

– Fałszerstwo komputerowe - określone jako umyślne wprowadzenie, dokonywanie jakichkolwiek zmian czy wykasowania lub ukrywania danych informatycznych, w wyniku czego powstaną dane nieautentyczne. – Oszustwo komputerowe - dokonane w sposób umyślny, powodując bezprawnie utratę majątku przez inną osobę poprzez wprowadzenie, dokonanie zmian, wykasowanie lub usunięcie danych informatycznych czy też każdą ingerencję w funkcjonowanie systemu komputerowego z zamiarem oszustwa lub nieuczciwym zamiarem uzyskania korzyści ekonomicznych dla siebie lub innej osoby.

Źródło: Konwencja Rady Europy o cyberprzestępczości, z dnia 23 listopada 2001 r. Budapeszt, Art. 7-8 www.prawo.pl/akty/dz-u-2015-728,18197508.html z dnia 20.08.2022 r.

Segment trzeci jest szczególnym zbiorem przestępstw ze względu na charakter zawartych informacji. Opisuje ów segment rzeczowo czwarta tabela.

Tabela 4. Tabela przestępstw ze względu na charakter zawartych informacji

– Przestępstwa związane z pornografią dziecięcą to: – przestępstwo o charakterze umyślnego i bezprawnego produkowania pornografii dziecięcej dla celów jej rozpowszechniania za pomocą systemu informatycznego. – przestępstwo oferowania lub udostępniania pornografii dziecięcej za pomocą powyższego systemu. – przestępstwo rozpowszechniania lub transmitowania dziecięcej pornografii za pośrednictwem systemu informatycznego. – przestępstwo pozyskiwania pornografii dziecięcej za pomocą systemu informatycznego dla siebie lub innej osoby. – przestępstwo posiadania pornografii dziecięcej w ramach systemu informatycznego lub na środkach do przechowywania danych informatycznych.

Źródło: Konwencja Rady Europy o cyberprzestępczości, z dnia 23 listopada 2001 r. Budapeszt, Art. 9, www.prawo.pl/akty/dz-u-2015-728,18197508.html z dnia 20.08.2022 r.

Przestępstwa związane z naruszeniem praw autorskich i praw pokrewnych są opisane w tabeli piątej.

Tabela 5. Tabela przestępstw związanych z naruszeniem praw autorskich i praw pokrewnych

– Każda Strona podejmie takie środki prawne i inne, jakie okażą się niezbędne dla uznania za przestępstwa w jej prawie wewnętrznym, naruszeń prawa autorskiego zdefiniowanego w prawie danej Strony zgodnie z podjętymi przez nią zobowiązaniami wynikającymi z Aktu Paryskiego z dnia 24 lipca 1971 roku zmieniającego Konwencję Berneńską o ochronie dzieł literackich i artystycznych, Porozumienia w sprawie handlowych aspektów praw własności intelektualnej oraz Traktatu Światowej Organizacji Własności Intelektualnej o prawach autorskich, z wyłączeniem praw osobistych przewidzianych przez te konwencje, jeżeli popełnione są umyślnie, na skalę komercyjną i za pomocą systemu informatycznego. – Każda Strona podejmie takie środki prawne i inne, jakie okażą się niezbędne dla uznania za przestępstwa w jej prawie wewnętrznym, naruszeń praw pokrewnych zdefiniowanych w prawie danej Strony, zgodnie z podjętymi przez nią zobowiązaniami wynikającymi z Międzynarodowej konwencji o ochronie wykonawców, producentów fonogramów i organizacji nadawczych zawartej w Rzymie (Konwencja Rzymska), Umowy w sprawie handlowych aspektów praw własności intelektualnej oraz Traktatu Światowej Organizacji Własności Intelektualnej o wykonaniach i fonogramach, z wyłączeniem praw osobistych przewidzianych przez te konwencje, jeżeli popełnione są umyślnie, na skalę komercyjną i za pomocą systemu informatycznego. – Strona może zastrzec sobie prawo do nie pociągania do odpowiedzialności karnej na podstawie ustępów 1 i 2 niniejszego artykułu w pewnych przypadkach, pod warunkiem, że istnieją inne skuteczne środki prawne oraz że zastrzeżenie to nie stanowi odstępstwa od międzynarodowych zobowiązań Strony określonych w międzynarodowych instrumentach, wymienionych w ustępach 1 i 2 niniejszego artykułu.

Źródło: Konwencja Rady Europy o cyberprzestępczości, z dnia 23 listopada 2001 r. Budapeszt, Art. 10, www.prawo.pl/akty/dz-u-2015-728,18197508.html z dnia 20.08.2022 r.

Eskalacja cyberprzestępczości i potencjał zysku przestępców, wykorzystujących strukturę okoliczności użyteczności technologicznej przez społeczeństwo, sprawia iż z samozorganizowanych przestępców, tworzone są siatki współdziałające ze sobą. Tworząc zorganizowaną przestępczość, dzielą się na poszczególne struktury wykonawcze i operacyjne. Specjalistyczne grupy sterujące procesem technologicznym, z użyciem tzw. "słupów" oraz rozmieszczone po wielu krajach jednostki wykonawcze, zarządzające mniejszymi strukturami, są coraz częstszym zjawiskiem. Największym skupiskiem przestępczości zorganizowanej wedle Europolu tereny Europy Wschodniej oraz Południowej. Charakteryzują się one wyjątkową aktywnością na tle cybernetycznym, o czym świadczą nieustanne działania i coraz częstsze próby dokonania cyberprzestępstw.[52] Szczególną ekspansją w obszarze cybernetycznym na terenie Rzeczpospolitej Polskiej charakteryzuje się Rosyjsko-Ukraińska grupa przestępcza, nieustępliwie dokonująca prób wyłudzeń o charakterze phishingowym, smishingowy, czy vishingowym.[53] Instytucją działającą na rzecz prowadzenia działalności naukowej w obszarze bezpieczeństwa cyfrowego jest zespół CERT Polska. Utworzony w ramach struktury Naukowej i Akademickiej Sieci Komputerowej (NASK), jest głównym działem Państwowego Instytutu Badawczego. W drodze implementacji ustawy z dn. 5 lipca 2018 roku o krajowym systemie cyberbezpieczeństwa, objął część kompetencji systemu zarządzania ryzykiem na poziomie krajowym.[54] Wśród nich wymienić należy najważniejsze działanie będące monitoringiem poszczególnych zagrożeń dla bezpieczeństwa w skali krajowej w obszarze cybernetycznym. Ponadto dokonywane są operaty szacunkowe możliwie występującego ryzyka w obszarze cyberbezpieczeństwa wobec którego podejmowane są wzmożone jego analizy. Ustawowo CSIRT zobowiązany jest do współpracy między zespołami MON, pod nadzorem Ministra Obrony Narodowej a także GOV, prowadzony przez Agencję Bezpieczeństwa Wewnętrznego. Przesyłane są również informacje o powstających incydentach stanowiących ryzyko owym podmiotom. Podmiot ten zobligowany jest do wydawania komunikatów dotyczących zidentyfikowanych zagrożeń w obszarze cyberbezpieczeństwa jak i reagowanie na te doń zgłoszone a także klasyfikacja ich wedle typologii zagrożenia. w CSIRT, bo tak obecnie nazywa się ów

[52] W. Pływaczewski, *Współczesne trendy przestępczości zorganizowanej w Europie (analiza wybranych zjawisk przestępczych z uwzględnieniem zadań Agencji Unii Europejskiej ds. Współpracy Organów Ścigania – Europol*, Olsztyn, 2021, s. 1
[53] Informacje uzyskane od Policjantów w drodze doświadczeń własnych z atakami phishingowymi
[54] Źródło: Nask, https://www.nask.pl/ z dnia 27.10.2022 r.

zespół, dokonywane są również badania w obszarze informatycznym celem wyszukiwania zagrożeń mogących objąć bezpieczeństwo publiczne lub narodowe. W tym celu tworzone są rekomendacje do zastosowania zarówno przez społeczeństwo jak i podmioty na wszelkich szczeblach administracyjnych. Operatywności dopełnia współpraca na arenie międzynarodowej, polegająca na wymianie informacji w obszarze zagrożeń, a także w obszarze identyfikacyjnym incydentów stanowiących potencjalne zagrożenia.[55] Informacje zarówno o raportach tworzonych w sektorze bezpieczeństwa informatycznego jak i poszczególnych rekomendacjach każdy obywatel Rzeczypospolitej Polskiej może uzyskać pod adresem strony https://www.nask.pl/

2.3. Problematyka funkcjonowania cyberprzestępczości

Przestępczość jest nieodłącznym społeczeństwu zjawiskiem od zarania dziejów. Motywy wpływające na zakres działań jednostek, od początku istnienia ram zasad funkcjonujących w społeczeństwach były uwarunkowane. Najczęściej występującymi motywami oczywiście były pobudki własne, motywy o tle ekonomicznym, politycznym czy psychologicznym. Jednostki ulegające swym emocjom, niesubordynowane, mające zaplecza w postaci towarzyszących im motywów, stanowią grupę która może potencjalnie dokonać czynów o przyjętym charakterze przestępczym. W procesie rozwoju społecznego, gospodarczego, zaś w końcu technologicznego, owe jednostki dokonujące przestępstw nieustępliwie towarzyszyły cywilizacji. W dobie dzisiejszych czasów, nieustannie rozwijającego się sektora cybernetycznego, jak wyżej można było zauważyć, liczba przestępstw rozwija się z roku do roku. Proceder ten możliwy jest dzięki niespójnemu prawu na tle międzynarodowym. Skala cyberprzestępstw jest ogromna, siatka zorganizowanych grup przestępczych wyspecjalizowana zaś relokacja poszczególnych jej tworów na terenach różnych państw, sprawia że poszukiwanie przestępców utrudniają niespójne działania w zakresie prawnym. Jak wynika z przeprowadzonych przeze mnie rozmów z Policjantami wydziału ds. przestępstw gospodarczych, trudność ta jest bardzo często wspominana w towarzystwie niejednolitej kooperacji służb na arenie międzynarodowej. Ponadto, problem stanowi kategoryzacja poszczególnych przestępstw w obszarze międzynarodowym. W wielu bowiem krajach świata zjawisko cyberprzestępczości jest ubogo przyjęta w procesach legislacyjnych. W innych zaś w ogóle nie występują. W państwach rozwiniętych, które rozwinęły prawne

[55] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa,(Dz. U. 2018 poz. 1560, Art.26 ust.1-3)

aspekty dotyczące cyberbezpieczeństwa, mają jednak niespójność wobec innych państw, co stanowi lukę uniemożliwiającą skuteczną współpracę między ich organami ścigania. Litera prawa na zasadzie Dura lex, sed lex[56], stanowi obszar niezgody kwalifikowalności poszczególnych czynów. Różnice prawne w wielu Państwach sprawiają utrudnienia w możliwości podjęcia działań śledczych w kooperowanym trybie.

Nadrzędnym dekretem stanowiącym proces implementacji prawnej na terenach krajów Unii Europejskiej jest Dyrektywa Parlamentu Europejskiego I Rady (Ue) 2015/2366 z dnia 25 listopada 2015 r. zwaną jako Payment Services Directive. Owa dyrektywa jest dziewięćdziesięcio trzy stronicowym dokumentem, mającym stanowić zakres norm i obowiązków dostawców usług na terenie Unii Europejskiej. Jako iż Polska do niej należy od 2003 roku, również i w naszym systemie prawnym musi ona być zaimplementowana. W drodze owej Dyrektywy objętymi zostają banki, podmiotów o charakterze instytucji płatniczych, podmioty oferujące karty sklepowe, karty paliwowe, czy też operatorzy bankomatów. Dyrektywa ta jest regulatorem warunków płatności elektronicznych, która została ogłoszona celem podniesienia bezpieczeństwa transakcji na terenie Unii Europejskiej. W swej zaktualizowanej formie PSD2, wymusza ponadto implementację dodatkowych zabezpieczeń kont bankowych. O ile dotychczas do zalogowania się na stronie bankowej wystarczył zaledwie login i hasło, o tyle po zmianach PSD2 ma być dodatkowy czynnik uwierzytelniający - kod przesłany w formie sms czy też wygenerowany w aplikacji danego banku na stronę którego chcemy się zalogować. Ponadto został skrócony czas bezczynności na stronie. Brak aktywności użytkownika, po pięciu minutach skutkować będzie automatycznym wylogowaniem z sesji. Choć zasadna zmiana, lecz dość nietypowa, wprowadziła w życie nowy wymóg. Mowa tu o potwierdzeniu kodem PIN średnio co piątą płatność kartą przy zakupach o wartości poniżej 50 złotych. Za istotną i w sumie bardzo racjonalną formą wprowadzenia dodatkowego bezpieczeństwa naszych środków, zainicjowano zmiany płatności internetowych z użyciem kart płatniczych. Jako iż dotychczas możliwe były one po wprowadzeniu numeru karty, kodu cvv i daty ważności karty, forma przekazania tak wrażliwych danych podmiotom, stanowiło poważne zagrożenie nadużyć czy też wycieku danych a w konsekwencji utraty środków

[56] Twarda reguła prawa rzymskiego, oznaczająca ścisłą nadrzędność prawa o niezbywalnym charakterze, traktującym konieczność stosowania się do obowiązującego na danym terenie prawa.

w przypadku kradzieży danych. Po korzystnych w mojej ocenie zmianach, ma być każdorazowo wprowadzone dodatkowe zabezpieczenie transakcji w postaci podania kodu potwierdzającego autoryzację transakcji wysłanego za pośrednictwem SMS-a bądź też poprzez potwierdzenie jej przez aplikację banku.[57] System płatności na terenie Rzeczypospolitej Polskiej jest również uregulowany w formie ustawy o usługach płatniczych ustanowionej w dniu 19 sierpnia 2011 roku. Ustawa ta jest dekretem prawnym, określającym jak czytamy w Art.1 oraz Art.2:

Art.1[58]

1. warunki świadczenia usług płatniczych, w szczególności dotyczące przejrzystości postanowień umownych i wymogów w zakresie informowania o usługach płatniczych;
2. prawa i obowiązki stron wynikające z umów o świadczenie usług płatniczych, a także zakres odpowiedzialności dostawców z tytułu wykonywania usług płatniczych;
   a) warunki wydawania i wykupu pieniądza elektronicznego;
3. zasady prowadzenia działalności przez instytucje płatnicze, małe instytucje płatnicze, dostawców świadczących usługę dostępu do informacji o rachunku, biura usług płatniczych, instytucje pieniądza elektronicznego i oddziały zagranicznych instytucji pieniądza elektronicznego, w tym za pośrednictwem agentów, oraz zasady sprawowania nadzoru nad tymi podmiotami;
4. zasady dostępu konsumentów do rachunku podstawowego;
5. zasady przenoszenia rachunków płatniczych prowadzonych dla konsumentów.

Art. 2. Ustawa określa również:[59]

1. podstawowe zasady funkcjonowania rynku krajowych transakcji płatniczych przy użyciu kart płatniczych;
2. zasady prowadzenia stron internetowych porównujących opłaty związane z rachunkiem płatniczym;
3. zasady funkcjonowania schematów płatniczych oraz zasady nadzoru nad tymi schematami.

[57] Źródło: Wikipedia, https://pl.wikipedia.org/wiki/Payment_Services_Directive z dnia. 27.10.2022 r.
[58] Ustawa o usługach płatniczych z dnia 19 sierpnia 2011 r. (Dz. U. 2011 Nr 199 poz. 1175 , Art.1)
[59] *Ibidem, Art. 2*

Rozwój technologii cyfrowej oraz wprowadzenie jej do użytku publicznego, jest niewątpliwie sukcesem postępu informatycznego. Dzięki nieustannych udoskonaleniach, programiści potrafią tworzyć środowisko wirtualne, do którego coraz większa ilość osób ma dostęp. Rozpowszechnienie technologii cyfrowej a także możliwość użytkowania z sieci, stanowił milowy krok w stronę postępu gospodarczo-społecznego, pozwalając na nawiązanie kontaktów, nabywanie wiedzy czy też dokonywania transakcji internetowych na całym świecie. Rzeczywistość cyfrowa obecna jest w życiu osób wszelkich pokoleń. W styczniu 2022 roku, liczba użytkowników korzystających z internetu wyniosła ponad 5,15 miliarda osób[60]. Szacuje się iż do roku 2030, liczba ta wzrośnie do 7,5 miliarda użytkowników przy zakładanej populacji 8,5 miliarda osób[61] Powszechność stosowanych możliwości przy użyciu aplikacji czy też stron internetowych w dobie dzisiejszych czasów nikogo nie dziwi. Wszak bowiem sprzęty typu smartfon czy komputer są nieodłącznym elementem dużej ilości osób. Oszczędność czasu jaką zaskarbiamy sobie dokonując płatności przez internet za dokonany zakup produktów czy też wysyłając wiadomości do znajomych, daje nam niezwykłą swobodę. Ów możliwość upraszczania życia jednak często pozbawia społeczeństwa czujności, gdyż ze swobody, bywa że popadamy w wygodę i bezmyślne dokonywanie powtarzalnych czynności. Wraz z upływem lat, środowisko technologiczne zmienia się jednak. Świadomość środowiska technologicznego, luk, błędów czy "back door[62]" pozostawionych w kodach systemowych lub aplikacji wydaje się być nadzwyczaj wykorzystywaną formą popełniania cyberprzestępstw. Za przykład może posłużyć proces sprzedaży produktu na stronie internetowej portalu ogłoszeniowego OLX. Zakładając iż zamieszczony przez nas produkt, przeznaczony do sprzedaży trafi na potencjalnego kupca, ten może poprosić nas o maila celem rzekomego sfinalizowania transakcji. Zadowoleni, ciesząc się ze sprzedaży produktu możemy stracić czujność. Na nasz e-mail może przyjść mail potwierdzający iż zakupiono od nas produkt, instruujący że musimy potwierdzić sprzedaż klikając w link. Tu zaczyna się proces wyłudzenia danych. Bez sprawdzenia poprawności adresu strony na którą nas przekierowuje odnośnik z oryginalną domeną, możemy paść ofiarą przestępstwa. Inicjatorzy phishingu często przekierowują nas na fałszywą strony np. DHL-u czy też strony ING, czyli tak zwane domeny phishingowe, podczas których w

[60] Źródło; Websiterating, https://www.websiterating.com/pl/research/internet-statistics-facts/#chapter-1 z dnia 27.10.2022 r.
[61] Źródło; Currentware, https://www.currentware.com/blog/internet-usage-statistics/ z dnia 27.10.2022 r.
[62] T. Szulc, *Wzmacniaj swoje bezpieczeństwo informatyczne*, Racibórz, 2018, s. 58

przypadku wypełniania poszczególnych okienek np. adres, nr. dowodu, czy też pesel lub dane logowania do Bankowości Elektronicznej, dane te niezwłocznie przechwytuje przestępca. Logując się w bankowości elektronicznej, owy sprawca niezwłocznie próbuje wypłacić wszelkie środki poprzez transgraniczne przelewy. By zmienić urządzenie bazowe, korzystając z procesu podawanych przez nas nadal danych, generowany jest błąd który sugeruje niepoprawne wpisanie kodu autoryzacyjnego na stronie. W przypływie euforii sprzedanego produktu a i często pośpiechu, często wpisywany ponownie kod oznacza pełny dostęp i zmianę urządzenia przez przestępcę. W efekcie chwilowej nieuwagi i braku czujności lub też wiedzy technologicznej, przestępca może dokonać złożenia wniosku o udzielenie internetowego kredytu, a tym samym zwiększyć pulę strat właściciela konta bankowego. Jedynym ratunkiem, który należy dokonać niezwłocznie, jest wówczas kontakt z infolinią banku celem zgłoszenia przestępstwa, poinformować policję i zastrzec dowód osobisty. Udogodnienia dzisiejszych czasów, sprawiają iż czujemy się zbyt pewni operowania w sieci, co prowadzi do lekkomyślności i braku podejrzliwości. Istotnym w sytuacji powszechnych ataków w obszarze cybernetycznym zatem wydaje się być działanie prewencyjne o charakterze edukacyjnym na ogólnokrajową skalę.

Cyberbezpieczeństwo obecnie przechodzi swój "renesans" na świecie. Zagadnienia w obszarze bezpieczeństwa technologicznego procesów cybernetycznych jest skomplikowanym zagadnieniem. Transformacja społecznych zachowań w świecie technologicznym, sprawia iż przestępczość zorganizowana odnajduje się w nowych, coraz to bardziej wyszukanych formach modus operandi. Na darknecie[63] rośnie zapotrzebowanie na szereg informacji wrażliwych, które to stają się celem powyższych organizacji. W dobie dostępu do skradzionych danych wrażliwych, mogą one w drodze zakupu bądź też układu generować zyski na poziomie milionów a nawet miliardów euro. Dlatego też tak kluczowym jest zapewnienie dostępu do edukacji społeczeństwu, by zwiększać świadomość zagrożeń czyhających podczas użytkowania internetu. Wiedza, daje nam swego rodzaju przewagę, pozwalającą nam na czujniejsze operowanie w świecie cybernetycznym, a także zabezpieczenie danych wrażliwych. Uzależnienie społeczeństwa od technologii jest w dobie dzisiejszych czasów bardzo zastanawiające. Średnio każdy internatuta przebywa dziennie aż XXX godzin w

[63] P. Siuda, *Między Globalnością a Lokalnością. Specyfika Handlu Narkotykami W Polskim Darknecie – Rekonesans Badawczy, [w:] Nowe Technologie Komunikacyjne – Nowe Wymiary Lokalności*, (red.) K. Stachura, s. 1

internecie. Warto zatem skutecznie dociekać do dostępnej wiedzy na sprawdzonych źródłach. Europejska Agenda Cyfrowa wprowadziła ku temu okoliczności, by realizować plany działania w dziedzinie edukacji cyfrowej na lata 2021–2027, w oparciu o którą dowiedzieć się można szeregu prowadzonych procesów na rzecz edukacji społeczeństwa.[64] Wśród istotnych i wartych uwagi stron, celem zdobycia wspomnianej wyżej edukacji w internecie, należy wyszczególnić:

- CSIRT NASK - Strona Instytutu Badawczego prowadzącego badania na rzecz cyberbezpieczeństwa oraz rejestrację i działania na rzecz zapobiegania incydentom. Ponadto stanowi kopalnię wiedzy ku rozwoju świadomości w obszarze zagrożeń w sieci.[65]
- OSE IT Szkoła - To zintegrowana platforma edukacyjna mająca w swoich zbiorach pokaźny szereg kursów w obszarze cyfrowym na różnych poziomach, od podstawowego, po zaawansowany. Powyższa daje możliwość nabrania wiedzy i poprawy świadomości w zakresie funkcjonowania technologii, cyfrowej operatywności, sztucznej inteligencji a także cyberbezpieczeństwa [66]
- Niebezpiecznik - Jest Polskim serwisem o charakterze społecznościowym, który w oparciu o analizę bezpieczeństwa w internecie, raportuje, analizuje i promuje informacje dotyczące właściwego postępowania w środowisku cybernetycznym. Dostępne są również obszerne szkolenia, edukujące w obszarze kompetencji cyfrowch[67]
- Zaufana trzecia strona - Podobnie jak wyżej, jest to Polska strona o charakterze informacyjnym w obszarach zagrożeń płynących z korzystania z sieci. Na owej stronie zamieszczone są również informacje dot. podstaw bezpieczeństwa, alerty czy też szkolenia pozwalające na poszerzenie swoich kompetencji.[68]

Ponadto, na zasadzie dostępności do wiedzy cyfrowej, realizowanych jest szereg kampanii edukacyjnych przez poszczególne banki. Do końca 2022 roku realizowane są również projekty edukacyjne w ramach finansowania ze środków Unii Europejskiej, pozwalające na pogłębienie kompetencji cyfrowych a tym samym sprawniejsze

[64] Źródło: European Education Area, https://education.ec.europa.eu/pl/plan-dzialania-w-dziedzinie-edukacji-cyfrowej-na-lata-2021-2027 z dnia 27.10.2022 r.
[65] Źródło: NASK, https://www.nask.pl/ z dnia 27.10.2022 r.
[66] Źródło: OSE IT Szkoła, https://it-szkola.edu.pl/ z dnia 27.10.2022 r.
[67] Źródło: Niebezpiecznik, https://niebezpiecznik.pl/ z dnia. 27.10.2022 r.
[68] Źródło: Zaufana Trzecia Strona, https://zaufanatrzeciastrona.pl/ z dnia 27.10.2022 r.

operowanie w świecie technologii cyfrowej. Wspomnieć należy iż środowisko naukowe w obszarze technologii cyfrowych jest niezwykle rozwinięte. Zarówno w bibliotekach jak i w sklepach internetowych, znajdziemy szeroką gamę literatury specjalistycznej, dzięki którym nabrać można świadomości w cyfrowym świecie. Warto zaznaczyć iż w wersji elektronicznej, niezawodnym instrumentem ku pogłębiania wiedzy jest niezastąpiony google scholar, pękający w szwach od zarówno Polskiej, jak i światowej literatury naukowej, dostępnej po wyszukaniu interesującej nas frazy. Tak obszerna gama możliwości edukacyjnych z pewnością stanowi istotny filar w realizacji procesu edukacyjnego społeczeństwa. Rozwój w branży technologicznej nieustannie postępuje, zatem kluczowym jest by nadążać za nim i stać się jego nieodłączną częścią.

2.4. Socjotechnika w działaniach cyberprzestępców

Cyberprzestępcy wymyślają coraz to nowsze sposoby na pozyskanie kluczowych danych, uzyskania dostępu do kont bankowych czy też informacji wspomagających rozplanowanie ataku na szerszą skalę. Żeby tego dokonać najczęściej wykorzystywane są narzędzia socjotechniki które pozwalają oszustom na często skuteczne przeprowadzenie ataku. Socjotechnika jest zestawem narzędzi o charakterze psychologicznym, wykorzystywanym w celu wprowadzenia innych osób w określony tok myślenia a także działania. Innymi słowy socjotechnika używana jest do osiągania określonych celów czy przez osobę ją stosującą, wobec adresata jej użycia. Określana jest również jako pewnego rodzaju manipulację ludzi, celem realizowania określonych czynności, wedle zamierzeń socjotechnika. Nie bez powodu, bowiem istnieją trzy fundamentalne filary stosowania socjotechniki. Należą do nich[69]

– Perswazja - jest sposobem postępowania prowadzącego do zmiany przekonań tudzież wpływu na określone zachowania osób wobec których jest stosowana.[70]
– Manipulacja - określone zachowania mające na celu wywołanie wpływu społecznego poprzez przeprowadzanie rozmowy, czy też działań celem nakłonienia innych do realizacji określonego przez nas celu[71]

[69] Źródło, Zrozumieć Polskę, http://www.zrozumiecpolske.pl/rodzaje-socjotechnik/ z dnia 28.10.2022 r.
[70] J. Warchala, *Formy perswazji, Wydawnictwo Uniwersytetu Śląskiego*, Katowice, 2019, s. 8
[71] P. Łukowski, *Manipulacja. Analiza terminologiczna, Studia z teorii wychowania*, 2017, s. 198

– Intensyfikacja lęku - jest mechanizmem określanym mianem zwiększenia poczucia lęku lub zagrożenia poniesienia konsekwencji celem podporządkowania sobie jednostki wobec której jest stosowany.[72]

Szereg zabezpieczeń w firmie może być określany mianem najwyższej jakości system bezpieczeństwa, jednakże mimo wszystko, dostęp mają do niego pracownicy firmy. Czynnikiem istotnym, który wpływa na wzrost ryzyka skutków niepożądanych jest właśnie czynnik ludzki. Już od dziesięcioleci socjotechnika wykorzystywana jest do pozyskiwania informacji istotnych, do realizacji przestępstwa tudzież oszustwa. Idealnym przykładem stosowania socjotechniki w celu uzyskiwania danych wrażliwych jest Kevin Mitnick. W swej książce zatytułowanej "Sztuka podstępu", opisuje szereg swoich doświadczeń a także praktyk wykorzystywania narzędzi socjotechnicznych, dzięki którym wcielał się w rolę wielu pracowników firm. W efekcie postępowania, dokonywał personifikacji swojej osoby, przygotowując się do rozmów z wybranymi pracownikami. Zawiłe i zróżnicowane sposoby ataków, wraz z użyciem swej wiedzy w obszarze technologii, pozwoliły mu na dostęp do danych wrażliwych, objętych szczególną ochroną.

Opisując sztukę ataków socjotechnicznych, na szczególną uwagę zasługuje historia Henry'ego oraz jego ojca. Spierając się o fakt nieodpowiedzialności podania numeru karty kredytowej w jedynej zaufanej firmie StudioVideo w której jego ojciec pozostawił w posiadanie owe dane, wywołało spór, kończący się zakładem o 50 dolarów. Podczas gdy Henry zadeklarował iż jest w stanie w ciągu pięciu minut zdobyć numer karty kredytowej za użyciem socjotechniki, postanowił podjąć zakład. Dzwoniąc na informację wypożyczalni i prosząc o jej numer oraz numer wypożyczalni Sherman Oaks. Po kolejnym telefonie do owej wypożyczalni Sherman Oaks, uzyskawszy nazwisko menedżera i jej numer zatelefonował do wypożyczalni w której jego ojciec miał rachunek. Podając się za menedżera Sherman Oaks, zadał pytanie "Czy wasze komputery działają? Bo nasze co chwilę się zawieszają". Informując tym samym o obecności jednego z klientów Studio Video pragnącego dokonać wypożyczenia kasety, wspomniał również o fakcie niemożności sprawdzenia w systemie komputerowym że jest zapisany do tejże firmy. Podając nazwisko ojca Henry prosząc o opisanie adresu,

[72] P. Pawełczyk, *Socjotechnika lęku – zastosowanie w XXI wieku*, Poznań, 2018, s. 1

numeru telefonu i daty otwarcia konta, poinformował o presji gromadzącej się kolejki klientów i pytając stanowczo, o numer karty i jej daty ważności, uzyskał dane. [73]

Powyższa historia ukazuje w sposób dosadny w jakim stopniu czynnik ludzki, może przy odpowiednio zastosowanym technikom socjotechnicznym doprowadzić do wycieku istotnych informacji, pozwalających na bezprawne użycie ich celem osiągnięcia korzyści. Istotną zatem jest edukacja w zakresie podnoszenia świadomości czyhających zagrożeń a także metod stosowanych przez socjotechników do wykorzystania potencjalnych ofiar. Regularne podnoszenie swoich kompetencji w powyższym obszarze stanowić może spoiwo najsłabszego ogniwa jakim jest wyżej ukazany czynnik ludzki. Jako iż ryzyko jest swego rodzaju zagrożeniem nastąpienia pewnych niekorzystnych zdarzeń, jego ocena powinna być regularnie stosowana do aktualizacji procedur bezpieczeństwa. Nie da się ukryć iż zdecydowana większość obecnie realizowanych ataków dokonywanych jest na tle finansowym. Powyższe bowiem widoczne jest w zmasowanych próbach phishingu, vishingu czy też smishingu w ostatnich latach na całym świecie. By odpowiednio przygotować się do obrony przed nimi np. w firmie, fundamentalnym czynnikiem decydującym finalnie o efektywności zabezpieczeń, jest ocena ryzyka potencjalnych zagrożeń jakie mogą nas spotkać. Pierwszym filarem jest ocena strat które w wyniku ataku są prawdopodobne w wystąpieniu. Dokonać tego można w poniższych punktach.[74]

1. Należy zatem hipotetycznie przyjąć że incydent danego typu ataku już wystąpił w firmie, a do jego usunięcia potrzebnych będzie trzech wyspecjalizowanych pracowników, których łączny czas przywrócenia funkcjonalności zajmie wstępnie cztery godziny.
2. Zakładając iż owym atakiem będzie wirus który poprzez niewiedzę, pobrał w załączniku do maila pracownik działu IT, uznajmy na potrzeby zobrazowania skalowalności wywołuje to jednodniowy paraliż infrastruktury sieciowej w firmie zatrudniającej łącznie 40 osób.
3. Przyjmując iż średni dzienny zysk firmy w wyniku kooperacji personelu to 40000 zł netto, roczny koszt pracownika działu IT to 72000 zł netto, możemy w szybki sposób oszacować ocenę ryzyka oraz strat.

[73] K. Mitnick, *Sztuka Podstępu,* Gliwice, 2003, s. 63-64
[74] M. Szeliga, *Certyfikowany Specjalista IT Security*, Kwidzyn, 2015, s. 85

4. Wobec powyższego przykładu dokonujemy poszczególnych obliczeń:[75]

4.1. Koszt roboczogodzin działu IT:

– 72000 zł netto : 365 dni = 197,26 zł netto

4.2. Mnożymy ilość godzin przez czas potrzebny do zażegnania zagrożenia oraz przez liczbę pracowników do tego potrzebnych:

– 197,26 zł netto * 4h * 3 pracowników = 2367,12 zł netto

4.3. Następnie liczymy straty potencjalnie wywołane w oparciu o średnią zysku gdy firma funkcjonuje normalnie i dokonujemy obliczeń zysku na godzinę i mnożymy przez czas awarii sieci:

– 40000 zł netto / 24h = 1666,67 zł netto

– 1666,67 zł netto * 4h = 6666,68 zł netto

4.4. Na tym etapie należy zsumować wszystkie koszty które w perspektywie czasu awarii dadzą nam obraz potencjalnych strat w wyniku wybranego na potrzeby przykładu awarii sieci:

– 2367,12 zł netto + 6666,68 zł netto =9033,80 zł netto

4.5. Oszacować potencjalne straty w ujęciu rocznym w przypadku nawracającego się zjawiska występowalności danego zagrożenia, mnożąc owe straty przez średnią ilość ataków konkretnego typu.

Zgodnie z powyższym istotnym elementem oceny ryzyka, jest określenie prawdopodobieństwa wystąpienia danego rodzaju zagrożeń w formie skalarnej od 0 do 10, gdzie:

– 0 - oznacza niewielkie straty,
– 5 - średnie straty
– 10 - bardzo poważne straty

W przypadku próby np. dostępu do konta użytkownika oraz wyświetleniem komunikatu o braku dostępu, wynik powinien wynosić 0. Jeśli zaś złamanie hasła dostępu możliwe jest poprzez metodę prób i błędów, przechwycenie czy też detekcję, należy przypisać temu zagrożeniu wartość 5. Najbardziej istotnym, w dziesięciostopniowej skali będącym maksymalnym zagrożeniem może być możliwość uzyskania pełnego dostępu do danych przez atakującego. W sposób adekwatny do powyższego, należy dokonać oceny stopnia trudności przeprowadzania ataków. Pozwoli to na skuteczne określenie

[75] *Ibidem, s. 86*

ich powtarzalności, a także określenie priorytetowych obszarów w których występują najwyższe poziomy zagrożenia.

Analizując powyższą przykładną formę ataku tylko jednego z typów zagrożeń, powyższa firma może stracić z wyliczeń 9033,80 zł netto. Należy jednak zaznaczyć iż pula strat może objąć również pośrednie uszkodzenia serwerowni, uszkodzenia sprzętów, utratę danych handlowych, osobowych czy płatniczych. Finalny koszt ryzyka wystąpienia ataku o charakterze Malware, może zatem opiewać w znacznie wyższe sumy, w zależności od skali uszkodzeń dokonanych podczas jego implementacji w systemie i rodzaju oprogramowania. Dlatego właśnie tak istotnym jest wprowadzenie w życie cyklicznych szkoleń personelu, stosownego zabezpieczenia sprzętów czy też wdrożenie procedur prewencyjnych w oparciu o analizy ryzyka.[76] Posiadanie zestawu działań na rzecz zwiększenia ochrony danych, jest zdecydowanie bardziej skuteczniejsze gdy są w sposób holistyczny dopracowane. Brak wdrożenia poszczególnych poszczególnych elementów procedury bezpieczeństwa, skutkować może zwiększeniem się ryzyka wystąpienia poważnych zagrożeń przy użyciu niezabezpieczonych luk. W dobie dzisiejszych czasów, zorganizowane grupy przestępcze, a także wyspecjalizowane jednostki, opracowują ataki o zautomatyzowanym charakterze. Poszczególne programy mogą być napisane w sposób wyszukujący poszczególnych luk stron, oprogramowania systemu firm czy też próbując dokonać zmasowanego logowania, mogą zawiesić funkcjonalność domeny. Procedury są określane poprzez pryzmat charakteru działania firmy, jej wielkości a także sektora w którym operuje. W zależności od możliwości operacyjnych danych podmiotów, ich skala działania może się różnić. Dla przykładu, firma technologiczna mająca w swoim posiadaniu ogromne zasoby danych, istotnie będzie zmuszona do stworzenia wielostronicowej procedury działań w każdym jej dziale na wypadek wystąpienia poszczególnych zagrożeń. W sektorze energetycznym, będącym elementem infrastruktury krytycznej, zakres działania prócz oczywistych procedur wewnętrznych, jest rozszerzony o politykę bezpieczeństwa i wymiany informacji z jednostkami administracyjnymi oraz służbami ds. bezpieczeństwa kraju.

By uniknąć niepożądanych zagrożeń które czyhają na użytkownika internetu, warto opracować ścieżkę postępowania, by przygotować się na poszczególne incydenty.

[76] *Ibidem, s. 98*

Choć nie jest to proste, opierając się na statystykach z Komendy Głównej Policji, uświadomić sobie należy iż skala zjawiska zagrożeń w cyberprzestrzeni rośnie z roku na rok. Warto zatem pamiętać o najważniejszych dziesięciu aspektach które zdecydowanie zwiększą poziom bezpieczeństwa. Na podstawie poniższej listy przedstawiane są one następująco:

Lista dziesięciu zasad securyzacji cyberprzestrzeni:[77][78]

1. Zwiększenie poziomu wiedzy w obszarze zagrożeń - dokonując regularnych kursów, tudzież wdrażając nabytą wiedzę w zakresie świadomości cyfrowego bezpieczeństwa, możliwe jest zidentyfikowanie rodzaju zagrożenia a także udaremnienie potencjalnego ataku.
2. Zachowanie szczególnej czujności - pozwoli na prewencyjną weryfikację materiałów, załączników czy też programów, upewniając się czy też dane w których jesteś posiadaniu, są bezpieczne.
3. Wdrożenie procedur o określonych zasadach funkcjonowania oraz standardach bezpieczeństwa - pozwalające na skuteczne działanie w przypadku wystąpienia incydentu. Mając etapowy proces działania podczas ataku na nasze stanowisko komputerowe, możliwe jest skuteczniejsze reagowanie na powstałe zagrożenia.
4. Wyposażenie stanowisk komputerowych w rekomendowane oprogramowanie o charakterze antywirusowym. - Wedle swoich obserwacji, spostrzegłem iż dokonywanych może być nawet kilkaset, a nawet kilka tysięcy prób uzyskania dostępu do komputera dziennie!
5. Nieustanne poszerzanie kompetencji - Niezwykle ważny element w dobie dzisiejszych czasów. Nieustannie bowiem technologia ewoluuje. Wraz z powstaniem nowych aplikacji, mogą im towarzyszyć również niedopatrzone luki wobec których warto być przygotowanym.
6. Zwiększenie poziomu bezpieczeństwa danych logowania - Jako iż zdecydowanie łatwiej jest zapamiętać krótkie hasła, warto jednak wzmocnić poziom zabezpieczeń zmieniając je na alfanumeryczne wraz ze znakami specjalnymi.

[77] *Ibidem, s. 104-116*
[78] Źródło: Coraz Lepsza Firma, https://www.corazlepszafirma.pl/blog/bezpieczenstwo-danych-firmy z dnia 28.10.2022 r.

7. Jedno hasło do jednego konta - W przypadku posiadania bardziej skomplikowanego hasła do głównego konta, zaznaczyć należy iż powinno się posiadać różne hasła do odrębnych kont. W przypadku przechwycenia jednego, pozostałe nadal będą bezpieczne.
8. Zastosowanie menedżera haseł - W przypadku posiadania większej ilości kont oraz stosowania się do zasady odrębności haseł służących do logowania, należy powziąć pod uwagę aplikacje o powyższym charakterze, dające silne zabezpieczenie. Dzięki menedżerom haseł możliwe jest szybkie i bezpieczne logowanie do poszczególnych kont, uprzednio zapisanych w nim. Do najskuteczniejszych należą obecnie Last Pass oraz Bitwarden, dostępne również w darmowej wersji.
9. Logowanie Dwuskładnikowe - Ważnym w dobie zmasowanych ataków phishingowych na operacje finansowe jest zabezpieczenie kont bankowych, profili społecznościowych a także dostępu do skrzynek mailowych kluczem U2F który to uniemożliwi dostęp do konta osobom nieuprawnionym.
10. Alternatywne działania - W przypadku gdy wiedza, umiejętności i narzędzia nie pozwalają na usunięcie powstałego zagrożenia, warto mieć możliwość niezwłocznego działania we współpracy z lokalną firmą zajmującą się danymi incydentami czy też znajomymi specjalizującymi się w wyżej wymienionym obszarze.

Dostępność opracowania w formie kodu technologii komputerowej stworzyła udogodnienie dla społeczeństwa całego świata. Wraz z jej rozwojem, od lat osiemdziesiątych XX wieku nieustannie towarzyszyć zaczęła atmosfera strachu. Powodem bowiem jest również możliwość stworzenia oprogramowania mającego wykorzystywać luki, uszkadzać sprzęty, czy też wykradać dane, za pośrednictwem wirusa który to napisany przez programistę może owych szkód dokonać. Warto zatem wyszczególnić najpowszechniejsze ataki technologiczne w sferze cyfrowej.

Robak Morrisa

Najbardziej znanym wirusem w historii jest “Robak” stworzony przez Roberta Morrisa, amerykańskiego informatyka który sparaliżował cały ówczesny internet. Mimo dobrych chęci zmierzenia rozmiaru ówcześnie funkcjonującego internetu.

Wykorzystując luki w usługach Sendmail czy też Finger, owy wirus powodował multiplikację, rozprzestrzeniając się zablokował On ponad 6000 komputerów, co stanowiło ponad około 10 procent światowego zasobu urządzeń podłączonych ówcześnie do sieci. Mimo iż w intencji Morrisa było ukazanie zagrożenia płynącego z możliwości transferowania wirusa między komputerami, efekt niestety stał się odwrotnym od zamierzonego.[79] Skutki "Robaka Morrisa" zablokowały możliwość dostępową większości administratorów. Dopiero zespół informatyków z Uniwersytetu Kalifornijskiego oraz Instytutu technologicznego w Massachusetts utworzył oprogramowanie niwelujące skutki powyższego wirusa.[80]

Atak na Blue Security

Stworzona przez firmę Blue Security darmowa forma oprogramowania o charakterze antyspamowym, miała za zadanie informować nadawców spamu iż odbiorca nie jest zainteresowany podobnymi treściami.[81] Stosując Blue Frog, użytkownicy mieli za cel pozbycie się ich adresu z list mailingowych natrętnych nadawców. Owy program również posiadał własny filtr Blue Security dla owych firm pozwalający na wykluczenie osób nie chcących otrzymywać spamu. Mając możliwość porównania swoich list oraz tych które przeszły proces filtracji osób nie chcących uzyskiwać treści o charakterze spamowym, w prosty sposób na zasadzie porównania obu list, dokonywano rozpoznania społeczności używającej oprogramowania Blue Security.[82] Mając na uwadze specyficzny błąd logiczny w strukturalnym założeniu oprogramowań względem siebie, doprowadziło to do przeprowadzonego na szeroką skalę ataku wykorzystującego owe niedopatrzenia. W wyniku masowych skarg przeciążone a w konsekwencji zablokowane zostały serwery. Firma Blue Security finalnie przegrała walkę z spamerami, zaś zmuszona nieustającymi atakami wycofała oprogramowanie.[83] Jak więc można zauważyć, sprytnie napisany kod, w efekcie wielu testów i godzin programowania może doprowadzić do poważnych komplikacji zarówno na arenie międzynarodowej jak i lokalnej. Podobne zagrożenia w dobie nieustającego rozkwitu postępu technologicznego są nadal prawdopodobne, stąd tak ważnym jest zwiększanie swojego poziomu edukacji w zakresie cyberbezpieczeństwa.

[79] *Ibidem,* M. Szeliga, *Certyfikowany Specjalista IT Security*, s. 17
[80] Źródło: Wikipedia, https://pl.wikipedia.org/wiki/Robak_Morrisa z dnia 28.10.2022 r.
[81] *Ibidem,* M. Szeliga, *Certyfikowany Specjalista IT Security*, s. 30
[82] Źródło: Wikipedia, https://en.wikipedia.org/wiki/Blue_Frog z dnia 28.10.2022 r.
[83] *Ibidem,* M. Szeliga, *Certyfikowany Specjalista IT Security*

Mając bowiem specjalistyczne umiejętności techniczne oraz wiedzę praktyczną jesteśmy w stanie skuteczniej odpierać ataki o niechcianym charakterze.

Rozdział 3. OBSZAR BADAŃ NAD CYBERPRZESTĘPCZOŚCIĄ

Procedowanie nad cyberprzestępczością jest niezwykle istotnym obszarem, niezbędnym do zapewnienia jak najwyższego poziomu bezpieczeństwa w strukturach funkcjonowania Państwa Polskiego. Aby dociec najbliższych informacji tudzież stanu faktycznego poruszanego zagadnienia, dokonane zostały badania polegające na przeprowadzeniu wywiadów w formie kwestionariuszowej z ekspertami w poszczególnych płaszczyznach cyberbezpieczeństwa. Powyższe mają na celu przybliżyć problematykę zagrożeń w Polsce, a także problematykę procesów legislacyjnych w Polsce. Charakter kwestionariusza został utworzony ku możliwości zinterpretowania zagadnień oraz wysnucie potencjalnych rozwiązań metodologicznych które to będą przyczynić się mogą do skuteczniejszego działania służb czy też instytucji na tle zwalczania cyberprzestępczości w Polsce.

3.1. Problematyka bezpieczeństwa cybernetycznego społeczeństwa

Wspomniane wyżej zjawisko narastającego trendu cyberprzestępczości na terenach Rzeczypospolitej Polskiej, ma charakter niezmienny. Przestępcy dokonują przewektorowania swoich działań na nowy, zmniejszający poziom ryzyka poniesienia konsekwencji obszar. Znaczący wzrost cyberzagrożeń jest równoznaczny z jednoczesnym występowaniem luk czy też niedoprecyzowanych uchybień prawnych, czego skutkiem jest wzmożenie wysiłków przestępców w obszarze cybernetycznym. Kluczowym zatem jest zrozumienie problematyki z punktu widzenia osób wykonujących czynności służbowe na rzecz zwalczania przestępczości w przestrzeni cyfrowej. Ich zrozumienie, analiza oraz interpretacja stanowić może bowiem szczególny kamień milowy ku przeprowadzeniu zmian mających usprawnić funkcjonowanie Krajowego Systemu Bezpieczeństwa, a tym samym i bezpieczeństwa samego społeczeństwa.

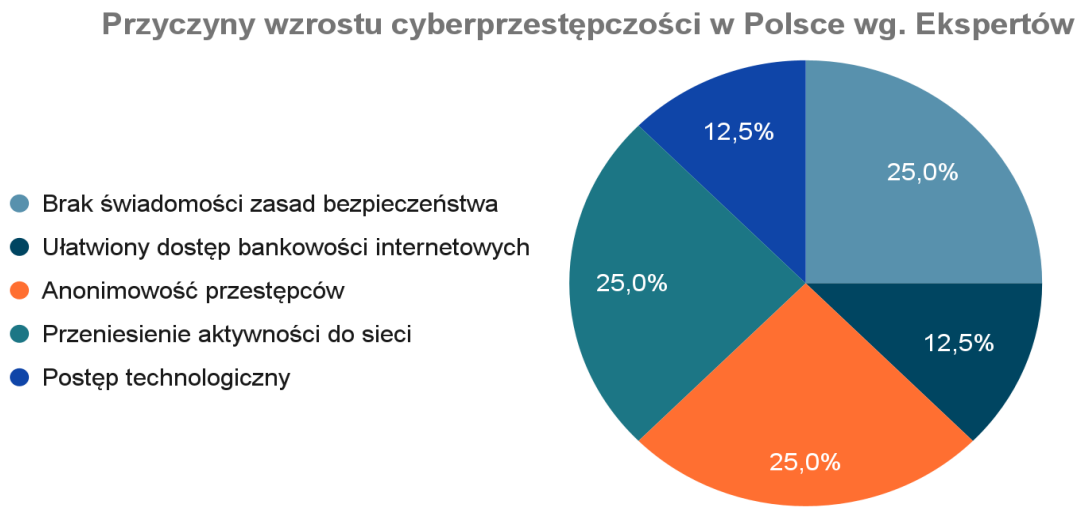
3.2. Analiza rezultatu ankiety badawczej

Kwestionariusz wywiadowczy został przeprowadzony wśród ośmiu ekspertów w poszczególnych branżach w obszarze cyberbezpieczeństwa. Powyższy wywiad przeprowadzony został wśród funkcjonariuszy Policji na trzech poziomach

wykonawczych: Funkcjonariusza szeregowego ds. walki z cyberprzestępczością, Naczelnika wydziału ds. walki z przestępczością gospodarczą oraz Dyrektorem Ministerstwa Obrony Narodowej. Ponadto przeprowadzony został wywiad z Biegłym sądowym w obszarze informatyki/biotechnologii a także wiceprezesem ds. innowacji technologicznej i prawnikiem jak i dwójką wykładowców specjalizujących się w obszarze informatyki śledczej jak i przestępstw w cyberprzestrzeni. Pytania zawarte w formularzach opierały się na ustaleniu przyczynowości eskalacji zjawiska cyberprzestępczości, wyznaczeniu najistotniejszych rodzajów zagrożeń a także ukazaniu proponowanych metod zapobiegawczych ich eskalacji. Ponadto podjęto starania w ustaleniu rodzajów zabezpieczeń, form reagowania przy wystąpieniu incydentu czy też określenia przeciążenia organów ścigania w związku z powiększającą się ilością przestępstw na tle cybernetycznym. Dokonano także rekonesansu działań specjalistów, detekcji słabych ogniw obszaru technologicznego oraz metod rozwoju cyberbezpieczeństwa w Polsce

Przeprowadzone badania w postaci kwestionariusza wykazały iż zjawisko trendu wzrostowego występowalności cyberprzestępstw w Polsce postępuje z kilku fundamentalnych przyczyn. Najczęściej wymienianym powodem wykazanym w wywiadzie z ekspertami jest brak fundamentalnej świadomości społeczeństwa w zakresie podstawowych zasad bezpieczeństwa prosperowania w cyberprzestrzeni. Za kolejny istotny czynnik wymieniono zaś poczucie anonimowości przez przestępców, czego efektem jest wzmożone działanie wobszarze cybernetycznym, w związku z nieuchwytnością ich działań. Ostatnim z elementów wymienianych jest postępujący trend przenoszenia swojej operatywności do rzeczywistości wirtualnej. Przez sam bowiem okres wybuchu pandemii jak omawialiśmy wyżej, był to istotny czynnik ekspansji zarówno społeczeństw całego świata, jak i przestępców do cyberprzestrzeni, co zwiększyło pulę popełnianych na tym obszarze przestępstw. Prócz powyższych wymieniono także ułatwiony dostęp do bankowości internetowej, co sugeruje iż w związku z uproszczeniem czynności operacyjnych transakcji bankowych, sprawiło iż na tym polu dość częstym były organizowane ataki phishingowe. Ponadto wspomniany został również postęp technologiczny, wobec którego nie wszyscy dorównują rozwojem wiedzy w powyższym obszarze.

Wykres 4. Przyczyny wzrostu cyberprzestępczości w Polsce wg. ekspertów



Źródło: Opracowanie własne w oparciu o przeprowadzony wywiad z ekspertami w formie kwestionariuszy.

3.3. Eksploracja obszaru cyberprzestrzeni – wywiad z ekspertami

Niezmiernie ważnym jest zrozumienie szerszego kontekstu problematyki obszaru cyberbezpieczeństwa w ujęciu poszczególnych służb. Realizując swoje kompetencje, codziennie zmierzać się muszą z bezpośrednimi czynnikami wpływającymi na ich skuteczność. By zrozumieć poszczególne jednostki a także wysnuć obszary w których można zaplanować obszary działań uskuteczniających poziom bezpieczeństwa, przeprowadzone zostały pytania które mogą przybliżyć środowisku naukowemu ku temu odpowiedź. Podążając w głąb analizy wyników ankiety badawczej, należało dokonać detekcji najczęstszych zagrożeń występujących w cyberprzestrzeni Polskiej. 100% Ekspertów z którymi został przeprowadzony wywiad, wykazała w formularzu iż głównym zagrożeniem dla obywateli Rzeczypospolitej Polskiej jest Phishing oraz jego odłamy o różnych modyfikacjach. Tak jednoznaczne odpowiedzi sugerują iż tego typu przestępstwo, ścigane z Art. 286 oraz Art. 287 kodeksu karnego są istotnym wektorem działań w obszarze którym muszą zostać podjęte środki prewencyjne jak i doraźne czynności redukujące cyberprzestępczość. Zmierzając dalej do zrozumienia problematyki przestępczości, istotnym celem było zrozumienie skali najniebezpieczniejszych zagrożeń jakie może sprowadzić działalność przestępcza w cyberprzestrzeni. W świetle odpowiedzi uzyskawszy szereg różnych opcji, zdefiniowano między innymi:

– Ataki na łańcuchy dostaw oprogramowania
– Phishing
– Hacking
– Stalking
– Szpiegostwo z wykorzystaniem nieautoryzowanego dostępu do danych służbowych
– Terroryzm
– Spoofing
– Włamania na rachunek bankowy
– Pedofilia

Tak szeroki zestaw przestępstw o groźnym charakterze wiąże się z próbą podjęcia konkluzji w temacie zastosowań możliwych do niwelowania ich występowalności. Powstaje zatem pytanie czy można wprowadzić udoskonalenia legislacyjne bądź proceduralne, pozwalające na przyspieszenie postępowania śledczego i wykrywania cyberprzestępców? W odpowiedzi, Biegły sądowy Piotr Maślanka udzielił zaskakującej wypowiedzi. Wnosi On bowiem iż warto byłoby wdrożyć poczynania w zakresie wezwania usługodawców dostarczających dostęp do sieci do identyfikacji adresu IP (cyfrowego numeru identyfikacyjnego urządzenia) należałoby powiązać z konkretnym obywatelem. Choć rozwiązanie to wydaje się być kontrowersyjnym, wydaje się iż usprawniłoby to identyfikację poszczególnych sprawców przestępstw, co w rezultacie mogłoby być szalenie skuteczne w praktyce. Wiceprezes ds. innowacji Mateusz Chrobok zaś poruszył inną kwestię. W świetle jego przekonań, istotnym byłoby poprawić charakterystykę pracy biegłych sądowych oraz poprawę jej warunków. Stosunkowo niskie dochody na owym stanowisku oraz zbyt duża odpowiedzialność jemu towarzysząca, sprawia iż potencjalni specjaliści niechętnie podejmują pracę w owym charakterze biegłego. Dyrektor Departamentu Cyberbezpieczeństwa Ministerstwa Obrony Narodowej, Dominik Rozdziałowski poruszył głębiej omawianą problematykę, według niego kluczowym czynnikiem przyspieszającym zdolności operacyjne jednostek śledczych jest ujednolicenie prawa międzynarodowego celem szybszej wymiany informacji. Powyższa inicjatywa jak wymaga również bowiem zmian w ustawie prawa telekomunikacyjnego. Implementacja powyższych, istotnie mogłaby przyczynić się do stworzenia skuteczniejszego środowiska prawnego, potrzebnego do współpracy organów na tle międzynarodowym.

Obecnie bowiem interpretacje prawne są zróżnicowane, zatem ich ujednolicenie w mojej ocenie byłoby niezwykle skutecznym działaniem na rzecz poprawy bezpieczeństwa międzynarodowego. Jak twierdzi Funkcjonariusz Policji do spraw walki z przestępczością gospodarczą, czynnikiem wpływającym na poprawę operacyjności funkcjonariuszy w działaniach śledczych byłoby zwolnienie banków z tajemnicy bankowej w przypadku zaistnienia przestępstwa na rachunku właściciela konta. Powyższe bowiem w dobie obecnego systemu prawnego jest możliwe tylko po wydaniu decyzji przez Sąd, dostępu do historii rachunków bankowych przez Policję. Niestety w przypadku zmasowanych ataków o charakterze phishingowym, powstają dwa główne problemy. Pierwszym jest niepraktyczność, z powodu często zatartych śladów w cyberprzestrzeni przez przestępców w momencie wydania takowej zgody na dostęp. Drugim zaś powodem jest przeciążenie ilością spraw których w towarzystwie wydawanych zgód Policji, sędziowie musieliby się podjąć. Pozostałe odpowiedzi jakie zostały poruszone dotyczyły głównie prewencyjnych metod zabezpieczenia się przed incydentami cyberprzestępczości. Wymieniono bowiem dostęp do informacji oraz prowadzenie kampanii edukacyjnej w społeczeństwie, mogącej uświadomić ludzi o zagrożeniach związanych z dostępem do cyfrowej przestrzeni. W kwestii problematyki na tle prawnym przyjęto przez respondentów iż istotnym jest silniejsze egzekwowanie Rozporządzenia Ogólnego o Ochronie Danych Osobowych (RODO). W towarzystwie odpowiedzi, zaproponowano również stworzenie czytelniejszego prawa. Jego uproszczenie bowiem przyczynić się może do szybszego i uproszczonego stanowiska sędziowskiego w jego egzekwowaniu. Stosowanie się do prawa i jego egzekwowanie jest jednym z filarów problematyki badawczej, jednakże kolejnym niemniej istotnym jest również rodzaj wdrożonych zabezpieczeń. Propozycje w tym zakresie według ekspertów wymienione zostały poniższe metody zabezpieczeń[84]:

– Weryfikacja dwuskładnikowa
– Segregacja danych wrażliwych i niewrażliwych
– Szkolenia zasobów ludzkich
– Wdrażanie procedur bezpieczeństwa
– Wdrożenie systemu Deep packet inspection
– Role-based access control
– Dokonanie pseudonimizacji danych

[84] Opracowanie własne w oparciu o wyniki wywiadów formularzowych z ekspertami

W przypadku gdy jednak dojdzie do niespodziewanego ataku ze strony cyberprzestępców niezmiernie istotnym jest by wiedzieć w jaki sposób postępować. Pytając o charakterystykę działania, koniecznego do podjęcia przez osoby poszkodowane, Eksperci udzielili kilka wskazówek, pozwalających na minimalizację poniesionych strat. W wyniku zadanego im pytania w powyższym obszarze, dokonać można wyciągnięcia następujących wniosków, ujętych w kilku punktach.

1. Jeśli incydent ataku cyberprzestępcy skierowany był do ataku w stronę konta bankowego, należy niezwłocznie zgłosić konieczność zablokowania wszelkich operacji na koncie. Dokonać tego należy na infolinii swojego banku lub też osobiście w lokalnej siedzibie.W pozostałych przypadkach, gdy nie zostały przejęte nasze dane osobowe, należy przejść do punktu trzeciego;
2. Następnie koniecznym jest zastrzeżenie dowód osobisty w urzędzie miasta jeśli w wyniku cyberataku zostały przejęte wrażliwe dane osobowe np. (nr dowodu, PESEL) a także w Biurze Informacji Kredytowej (BIK) i bankach że istnieje możliwość wyłudzenia kredytu na nasze dane osobowe;
3. Istotnym jest by zabezpieczyć konwersację z przestępcą jeśli takowa nastąpiła i zebrać dostępne naszym możliwościom informacje które mogą przyczynić się do skuteczniejszego złapania sprawcy;
4. Kolejnym krokiem jest niezwłoczne udanie się na Policję, celem zgłoszenia incydentu i wszczęcia postępowania przygotowawczego śledztwa;
5. W miarę możliwości wesprzeć organy ścigania, przedkładając nowe materiały dowodowe;

Występowalność cyberprzestępstw zarówno w Polsce, jak i na świecie jest coraz większym problemem z racji bardzo dochodowego procederu, a także zwiększonej skuteczności działań na tle sprzyjającej koniunktury społeczno - prawnej. Mając na uwadze skalę zjawiska, organy ścigania nieustannie wszczynają nowe sprawy i poczynają postępowania przygotowawcze, czego skutkiem jest wydłużenie czasu śledztwa przez przeciążenie jednostek. Wedle Ekspertów osłabienie czujności wśród pokrzywdzonych, jest czynnikiem ułatwiającym dokonanie przestępstwa. W konsekwencji czego podawane są dane kart bankomatowych, numeru PESEL czy realizowana jest autoryzacja transakcji bez uprzedniego zapoznania się z wyświetlanymi komunikatami. Dodatkowym zjawiskiem utrudniającym wykrycie

sprawców jest poczucie wstydu bycia ofiarą cyberprzestępstwa. Brak zgłoszeń w takim przypadku do organów ścigania zawęża a w niektórych przypadkach również uniemożliwia dokonanie skutecznego śledztwa. Istotną rolę zatem w prewencyjnym zwalczaniu cyberprzestępczości wydaje się być edukacja. Podniesienie kompetencji i świadomości potencjalnych zagrożeń, skutkować może zahamowaniem a być może i zmniejszeniem skali zjawiska. Warto byłoby się zastanowić zatem czy w skutecznym działaniu nie warto by było wspomóc wydziały i służby. Jak zatem mają się one i czy mają dość jednostek ds. śledzenia i zwalczania cyberprzestępczości? Problematyka organizacji służb jak wynika z odpowiedzi Ekspertów polega na niedostatecznie posiadanym poziomie wiedzy i kompetencji w obszarze cybernetycznym. Wspomniane już niskie zarobki w stosunku do sektora prywatnego, nie zachęcają do pracy w szeregach państwowych. W województwie Podkarpackim jest zaledwie trzech policjantów ds. walki z cyberprzestępcami. Ewentualne braki kadrowe wywołane natłokiem spraw, powodują konieczność implementacji wsparcia biegłych sądowych. Reasumując owy konspekt, należy wspomnieć iż przesilenie ilością incydentów wśród społeczeństwa, omawiane jednostki są niedostatecznie wyposażone w specjalistyczne zasoby ludzkie. Powstaje zatem kolejny odłam przeciążenia systemu organów ścigania, zmniejszając tym samym skuteczność operacyjną ich działań. Kolejnym poruszanym zagadnieniem w formularzu jest pytanie w zakresie technologicznym, dotyczącym najsłabszego ogniwa urządzeń elektronicznych. Zrozumienie problematyki bezpieczeństwa technologicznego, pomoże bowiem na zwiększenie uwagi i w konsekwencji podjęcia debat naukowych w obszarze jego problematyki Wedle specjalistów udzielających wywiadu, najsłabszym ogniwem użyteczności technologii w społeczeństwie są niedostatecznie zabezpieczone systemy, deaktualizacja baz oprogramowań antywirusowych oraz brak bieżącego aktualizowania ich. Brak usprawnionych funkcjonalności czy też baz danych wirusów, skutkuje bowiem wykorzystania owych niekompletnych podatności przez cyberprzestępców. Warto wspomnieć również iż najważniejszym ogniwem w dobie obecnych czasów jest człowiek. Dokonując utworzenia zaplecza zasobów ludzkich, operujących w zakresie swoich kompetencji cyfrowych, możliwe w wystąpieniu są zaniedbania, przeciek danych i informacji wrażliwych a także w konsekwencji usterki czy też luki w zabezpieczeniach. Jak wynika z odpowiedzi, w przypadku wystąpienia ataku hakerskiego, skierowanego na urządzenie elektroniczne, serwer czy chmurę danych,

powinno się zastosować do procedur bezpieczeństwa. O ile sposób postępowania procedur bezpieczeństwa znacząco będzie się różnił w różnych sektorach, np. energetycznym, bankowym czy usługowym, to jego realizacja jest niezbędna do zminimalizowania strat a także niezwłocznego przywrócenia funkcjonowania systemu. Powyższe powinny być jednak przeprowadzane przez wykwalifikowany personel, wyspecjalizowany w branży IT oraz przeszkolony do interwencyjnego podejmowania działań w obszarze cyberbezpieczeństwa. W oparciu o odpowiedzi na pytanie w owym obszarze, utworzone zostało siedem zaproponowanych etapów reagowania które to w ujęciu ogólnym przedstawiają poniżej wymieniona lista działań:[85]

1. Przygotowanie procedur bezpieczeństwa - Etap ten pozwala na przygotowanie się w formie proceduralnej i zapoznanie poszczególnych pracowników z kolejnością reagowania w przypadku wykrycia incydentu w cyberprzestrzeni.
2. Wykrycie incydentu - jest niezwykle ważnym etapem. Dzięki zidentyfikowaniu rodzaju zagrożenia, można bowiem wysnuć potencjalne skutki ataku a także sposób jego działania. Ponadto pozwala nam na dostosowanie narzędzi do rodzaju incydentu, celem skutecznego minimalizowania strat a tym samym usunięcie zagrożenia.
3. Zastosowanie metod zabezpieczenia śladów - to etap pozwalający na identyfikację dowodów oraz ich archiwizację w zależności od systemu, platformy, serwera, chmury czy też urządzenia. Ku temu niezbędne jest bowiem w niektórych przypadkach dokonanie współpracy z organami ścigania czy też dostawcą usług
4. Analiza powłamaniowa - Pozwala na ocenę skutków zagrożenia, wysnucie stosownych wniosków, wykrycie luk czy też wzmocnienia procedur bezpieczeństwa po dokonanym ataku.
5. Przywrócenie z backupu, łatanie podatności - Na tym etapie dokonywane jest przywrócenie funkcjonalności urządzenia było celem ataku. Przywrócenie danych z kopii zapasowej pozwala na bezstratne dalsze operowanie sprzętu. Wskutek incydentu, winny być bowiem wykryte i naprawione najsłabsze ogniwa, które pozwoliły na przeprowadzenie ataku.
6. Testy akceptacyjne - Po dokonaniu łatania podatności, należy przeprowadzić symulowane ataki oraz testy podatności, pozwalające na określenie stopnia

[85] Opracowanie własne w oparciu o przeprowadzony wywiad z ekspertami

bezpieczeństwa.

7. Przywrócenie funkcjonalności jest ostatnim elementem działań, pozwalającym na powrót do prawidłowego kontynuowania pracy operacyjnej.

   Ścisła kooperacja specjalistycznych jednostek specjalistycznych w obszarze cyberbezpieczeństwa jest niezbędna do skutecznego niwelowania zagrożeń na tle technologicznym. Będąc specjalistą w obszarze cybersecurity, należy przede wszystkim dokonać rekonesansu wśród najczęściej występujących zagrożeń.

Pytając o powyższe ekspertów, zwrócili szczególną uwagę na kilka kluczowych kwestii:

1. Każdy specjalista w obszarze technologicznym jest również człowiekiem podatnym na słabości. W związku z kompetencjami jakie wykonuje, może On ulec szczególnie atrakcyjnej ofercie Hakerów, która przyczyni się do wycieku tudzież ułatwienia danych lub ściśle strzeżonych informacji;
2. NordVPN - czyli usługa dostępu do globalnej sieci z ukryciem adresu IP, jest dość problematyczną składową, przyczyniającą się do maskowania ataków przez poszczególne jednostki przestępcze.
3. SIEĆ TOR - czyli przeglądarka pozwalająca na szyfrowanie przepływu cyfrowych informacji i przesyłanie ich poprzez sieć węzłów, co uniemożliwia identyfikację przez dostawcę przeglądanych treści
4. Gwałtowny proces rozwoju technologicznego - sprawiający iż niektóre jednostki niestety w wyniku korzystania z archaicznych rozwiązań w stosunku do pędu technologicznego, będą podatne na ataki cyberprzestępców.

Ataki przeprowadzane są w różnoraki sposób, jednak najbardziej kluczowym w potencjalnych stratach według respondentów są Phishing i DDOS-DOS. Phishing tak naprawdę za użyciem dobrze przygotowanej socjotechniki w wykonaniu przestępcy, jest najgroźniejszym zjawiskiem. Mając na uwadze charakter działań, przełamywane bowiem są nie kody oprogramowania a ludzie. Emocje które starannie sterowane pozwolą socjotechnikowi na wprowadzenie ofiary w określony stan, powodują w wielu przypadkach jak wskazują statystyki Komendy Głównej Policji najczęstsze przyczyny strat i przeciążenia systemu. Kolejnym omawianym atakiem jest DDOS oraz DOS, który to ukierunkowany jest na złamanie zabezpieczeń oprogramowania systemów

celem wyrządzenia znaczących strat. Sklasyfikowane zagrożenia winny być objęte poszczególnymi procedurami działania. Jak zapewniają Eksperci, ich klasyfikacja wynika bowiem ze zróżnicowanych metod postępowania, dostosowanych do danego źródła zagrożenia. Brane bowiem pod uwagę są zarówno skala ataku oraz potencjalnych zagrożeń jakie ze sobą niesie. W zależności od charakteru funkcjonowania organizacji, implementowane są różne systemy procedur bezpieczeństwa. Do oceny owych podatności stosowane są:

– Common Vulnerability Scoring System CVSS - jest systemem określającym skalę podatności na zagrożenia i powagi luk która pozwala na dokonanie poczynań w określeniu priorytetów i działań.[86]
– Common Vulnerabilities and Exposures (CVE) będący instrukcją nadającą możliwą identyfikację zagrożeń i podatności[87]
– Common Weakness Enumeration (CWE) jest instrukcją określającą kategorię słabości (weakness) mogących wystąpić na danym sprzęcie[88]

By uniknąć wielu następstw powstających w wyniku ataków hakerskich czy też działań przestępczych, należy skłonić się ku refleksji, który sektor technologiczny wpłynąć może na poprawę zabezpieczeń sprzętów elektronicznych.

W odpowiedzi na to wymieniono następujące propozycje:

– Wsparcie innowacji technologicznych oraz edukacja w zakresie ich obsługi
– Wsparcie sektora bezpieczeństwa w obszarze bankowości elektronicznej
– Rozwój Sztucznej Inteligencji (AI)
– Wdrożenie edukacji w obszarze cyberbezpieczeństwa w społeczeństwie
– Rozwój informatyki śledczej celem skuteczniejszego wykrywania sprawców
– Rozwój technologii zabezpieczeń chmur obliczeniowych

Wsparcie bowiem poszczególnych sektorów pozwoli zrozumieć postępującą technologię a tym samym możliwość jednoczesnego wdrażania najnowocześniejszych systemów bezpieczeństwa. Ponadto wraz z dostępem do innowacyjności, możliwe

[86] Źródło: Wikipedia, https://en.wikipedia.org/wiki/Common_Vulnerability_Scoring_System z dnia 29.10.2022 r.
[87] Źródło: Javaheri, https://javaheri.pl/co-to-jest-cve-i-czemu-warto-zglaszac-podatnosci/z dnia 29.10.2022 r.
[88] Źródło: Whitehats https://whitehats.pwr.edu.pl/research/podatnosci-wstep/ z dnia 29.10.2022 r.

będzie przeprowadzenie szkoleń mających na celu podniesienie kompetencji zarówno społeczeństwa, by zaszczepić w nim świadomość zagrożeń, jak i specjalistów owe zagrożenia zwalczających. Dokonywanie powyższych wdrożeń jednak może nie wystarczyć, należy bowiem przeprowadzać cyklicznych predykcji w obszarze czyhających zagrożeń w cyberprzestrzeni. Jako iż technologia jest niezwykle szybko rozwijającym się sektorem, należy zwrócić uwagę iż przeprowadzane są coraz to nowe projekty badawcze nad tworzeniem coraz to bardziej zaawansowanych jej form. Sztuczna inteligencja (SI) wydaje się zatem być to ogromną szansą na optymalizację wszelkich procesów w których można ją zaimplementować. SI lub AI (artificial intelligence), definiowana jest jako systemy lub zaawansowane maszyny które dzięki swoim możliwościom naśladują ludzką inteligencję wykonując określone zadania w oparciu o posiadane informacje (dane).[89] Na horyzoncie mamy również komputery kwantowe które mogą dokonywać Jego powstanie przyczynić się może do istnego wstrząsu w sektorze technologicznym. Moc komputera kwantowego jest oparta na specyficznych obliczeniach kwantowych, mogących wyprzedzić moc najszybszego superkomputera o ponad 150 milionów razy. Czym na ten moment martwią się specjaliści? Jak wynika z odpowiedzi kwestionariusza, obszary w stronę których winniśmy na ten moment zwrócić swoją uwagę to:

- Ewoluujący trend metodyki stosowania phishingu;
- Public Key Infrastructure (PKI) - który to ustanawia obszary między innymi weryfikacji tożsamości użytkowników czy też realizuje szyfrowanie przekazu lub certyfikacji;
- Infrastruktura zabezpieczeń bankowych z racji dalszej ekspansji ataków na środki zgromadzone na kontach ich właścicieli;
- Każde inne technologie które można wykorzystać w celu dokonania przestępstwa.

[89] Źródło: Strona Oracle, https://www.oracle.com/pl/artificial-intelligence/what-is-ai/ z dnia 29.10.2022 r.

Zakończenie

W dobie niezwykle szybko rozwijającej się innowacyjności a także powszechnego dostępu do technologii, skala zjawiska cyberprzestępczości jest wprost proporcjonalnie odwrotnym wyznacznikiem poziomu bezpieczeństwa. Cyberprzestrzeń nieustannie jest atakowana przez zautomatyzowane oprogramowania dokonujące prób przechwycenia danych zaś w asyście hakerów i różnego typu przestępców, operując w sieci nie można czuć się całkowicie bezpiecznie. Zmasowane ataki phishingowe przeprowadzone na całym świecie a także szereg ofensyw hakerskich na poszczególne jednostki administracji rządowej czy też w sektor prywatny, sprawia iż dane winny być coraz lepiej chronione. Implementacja procedur działań, opartych gruntowną analizą zagrożeń możliwych w wystąpieniu. Szereg uwarunkowań prawnych, mimo iż powołują do działania poszczególne organy składające się na Krajowy System Cyberbezpieczeństwa i są aktualizowane, to zaniedbanie podstawowych błędów organizacyjnych na tle prawnym stwarzają duże ryzyko niekompatybilności działań służb. Brak jednolitego prawa na arenie międzynarodowej w cyberprzestrzeni, powoduje szereg komplikacji w dokonywaniu skutecznej współpracy między organami ścigania. Istotnym jest również doposażenie służb Policji w nowe szeregi specjalistów z branży technologicznej, by przeprowadzać skuteczniejsze postępowania śledcze. Kluczowym również jak zaznacza jeden z Ekspertów, wydaje się niedostateczne finansowanie powyższych stanowisk. Zbyt mała ilość specjalistów składa się na efekt przeciążenia organów ścigania oraz niedostatecznie kompetentnego wykonywania powierzonych zadań. Podobnie jak w przypadku Policji, również i organy władzy sądowniczej borykają się z nadmierną ilością spraw cyberprzestępstw w Polsce. Mimo iż w roku 2015 liczba sędziów w Polsce wynosiła 10.000 wakatów, to obecnie oscyluje w okolicach 1000 stanowisk[90]. W porównaniu z ilością samych spraw cyberprzestępstw które przypadają rocznie na jednego sędziego to ilość 83[91] spraw do zasądzenia, stanowi duży problem. Na domiar obowiązków spoczywa bowiem jeszcze wydawanie werdyktów orzeczeń, analiz ekspertyz, przesłuchiwanie świadków i szereg innych czynności, w tym wydawanie zezwoleń na uchylenie tajemnicy bankowej wobec prowadzonych przez Policję postępowań w sprawie śledztwa oskarżonych o phishing.

[90] Źródło: Justitia https://www.iustitia.pl/dzialalnosc/opinie-i-raporty/4318-raport-iustitii-o-statystykach-wymiaru-sprawiedliwosci z dnia 29.10.2022 r.
[91] Wyliczenia własne w oparciu o dane uzyskane od Komendy Głównej Policji, Warszawa z dnia 21.04.2022 r.

Nadmierne obciążanie biegłych odpowiedzialnością, w porównaniu do poziomu zarobków uzyskanych w drodze wydawania ekspertyz, stanowi barierę odpychającą szereg specjalistów od pracy asystującej wymiarowi sprawiedliwości. Należy wziąć pod uwagę powyższe i wystosować szereg działań usprawniających organizację pracy poszczególnych jednostek służb Policyjnych a także Wymiaru Sprawiedliwości jak i podległym im stanowisk. Chcąc dokonać zmian o charakterze ogólnym w społeczeństwie, niezbędnym jest wdrożenie szkoleń w obszarze technologicznym na szeroką skalę, by społeczeństwo uzyskawszy świadomość z czyhających zagrożeń związanych z użytkowaniem technologii cyfrowej, było przygotowane na potencjalne ataki.

Wnioski

Opierając się na dostępnych mi publikacjach, wywiadach z Ekspertami służb Policji, Ministerstwa Obrony Narodowej a także Wymiaru Sprawiedliwości, dokonałem przemyśleń ku wyciągnięciu poniższych wniosków priorytetowego przedmiotu działań. Należą do nich:

- Wsparcie finansowe służb Policji, umożliwiające stworzenie warunków atrakcyjnych dla specjalistów chcących za rozsądne wynagrodzenie podjąć się służby Ojczyźnie.
- Wspieranie procesu aplikacji sędziowskich, umożliwiających uzupełnienie niedostatecznie rozbudowanej kadry wymiary sprawiedliwości.
- Zwiększenie honorarium biegłych sądowych współmiernie do pokładanych w nich obowiązków
- Niezmiernie ważnym jest wdrożenie inicjatyw bądź działań zmierzających do ujednolicenia definicji i prawa międzynarodowego w obszarze cyberprzestrzeni.
- Wsparcie struktur współpracy międzynarodowej jednostek organów ścigania ku sprawniejszym przeprowadzeniu śledztwa cyberprzestępców
- Wsparcie innowacji technologicznych mających na celu poprawę bezpieczeństwa oraz gruntowna analiza potencjalnych możliwości użycia w celu przestępczym dostępnych technologii
- Dokonywanie predykcji kierunków rozwoju technologicznego przy bieżącym jego monitorowaniu

Bibliografia

1. Siwicki M., Podział i definicja cyberprzestępstw, Materiały Szkoleniowe, [b.m.w.], 2012.
2. Dworakowski W., Zarządzanie bezpieczeństwem informacji wg normy BS 7799 – Wprowadzenie, Kościelisko, 2005.
3. Szeliga M., Certyfikowany Specjalista IT Security, Kwidzyn, 2015.
4. Jaroszewska I. A. , KPP Monografie Wybrane aspekty przestępczości w cyberprzestrzeni Studium prawnokarne i kryminologiczne, Olsztyn, 2017.
5. Pływaczewski W., Współczesne trendy przestępczości zorganizowanej w Europie (analiza wybranych zjawisk przestępczych z uwzględnieniem zadań Agencji Unii Europejskiej ds. Współpracy Organów Ścigania – Europol, Olsztyn, 2021.
6. Pawełczyk P., Socjotechnika lęku – zastosowanie w XXI wieku, Poznań, 2018
7. Mitnick K., Sztuka Podstępu, Gliwice, 2003.
8. Wydro K. B., Telematyka – znaczenia i definicje terminu, [w:] Telekomunikacja i techniki informacyjne 1-2/2005, [b.m.w], 2005.
9. Resztak I., НАУКОВИЙ ВІСНИК 4’ Львівського державного університету внутрішніх справ, Львівського , [b.m.w.], 2011.
10. Szulc T., Wzmacniaj swoje bezpieczeństwo informatyczne, Racibórz, 2018.
11. Siuda P., Między Globalnością a Lokalnością. Specyfika Handlu Narkotykami W Polskim Darknecie – Rekonesans Badawczy, [w:] Nowe Technologie Komunikacyjne – Nowe Wymiary Lokalności, (red.) K. Stachura, [b.m.r.w.].
12. Juszczak A., Rys Historyczny Przestępczości, [w:] Security, Economy & Law Nr 1/2018 (XVIII), (74–85) DOI 10.24356/SEL/18/4.
13. Chaliand G., Blin A., Historia Terroryzmu, Od starożytności do Da'isz w przekładzie na j. Polski Katarzyny Pachniak, [b.m.w.], 2020.
14. M. Grzelak, K. Liedel, Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski – zarys problemu, [b.m.r].
15. Kosiński J., Paradygmaty cyberprzestępczości - Wstęp, [b.m.w.], 2015.
16. Rzeczpospolita Polska, Ministerstwo Administracji i Cyfryzacji, Agencja Bezpieczeństwa Wewnętrznego, Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej, Warszawa, 25 Czerwca 2013.

17. Ministerstwo Cyfryzacji, Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022, Warszawa, 2017.
18. Wasilewski J., Cyberprzestępczość - Wybrane Aspekty Prawnokarne I Kryminalistyczne, Uniwersytet W Białymstoku Wydział Prawa, Białystok, 2017.
19. Mazur S., Zagrożenia bezpieczeństwa danych w lokalnych sieciach komputerowych – ataki i metody obrony, Karkonoska Państwowa Szkoła Wyższa w Jeleniej Górze, Jelenia Góra, [b.r.w.].
20. Warchala J., Formy perswazji, Wydawnictwo Uniwersytetu Śląskiego, Katowice, [b.m.w.], 2019.
21. Łukowski P., Manipulacja. Analiza terminologiczna, Studia z teorii wychowania, [b.m.w.], 2017.
22. Sysło M. M., Technologia Informacyjna w edukacji, [w:] Poradnik dla nauczycieli informatyki w gimnazjum(18), Uniwersytet Wrocławski, Wrocław, [b.r.w.].
23. Kołodziejczyk R., Nowa Odsłona Terroryzmu – Cyberterroryzm, [w:] Rocznik Bezpieczeństwa Międzynarodowego 2017, vol. 11, nr 2, Wydział Prawa, Administracji i Zarządzania Uniwersytetu Jana Kochanowskiego w Kielcach, Kielce.
24. Danielewicz Z., Zeszyty Naukowe Wydziału Elektroniki i Informatyki Politechniki Koszalińskiej, Koszalin, 2018, Nr 13.
25. Związek Banków Polskich, Raport ZBP Cyberbezpieczny portfel, Edycja III, [b.m.w.], 2020.
26. Santander Consumer Bank, Raport Polaków Portfel Własny Bezpieczni na e-zakupach, [b.m.w.], 2022.
27. Santander Consumer Bank, Raport Polaków Portfel Własny, Polacy na e-zakupach, [b.m.w.], 2021.
28. Raport roczny z działalności CERT Polska, Krajobraz bezpieczeństwa polskiego internetu 2021, Warszawa, 2021.
29. NASK PIB/CERT Polska, Krajobraz bezpieczeństwa polskiego internetu, Raport roczny
z działalności CERT Polska, Warszawa, 2020.

30. Komunikat Komisji do Parlamentu Europejskiego, Rady oraz Komitetu Regionów z dnia 22.5.2007, Kom(2007) 267 wersja ostateczna, 2007, Bruksela.
31. Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. 1997 nr 78 poz. 483).
32. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, (Dz. U. 2018 poz. 1560).
33. Ustawa o usługach płatniczych z dnia 19 sierpnia 2011 r. (Dz. U. 2011 Nr 199 poz. 1175).

Netografia

1. https://education.ec.europa.eu/pl/plan-dzialania-w-dziedzinie-edukacji-cyfrowej-na-lata-2021-2027 z dnia 27.10.2022 r.
2. https://www.gov.pl/web/cyfryzacja/krajowy-system-cyberbezpieczenstwa- z dnia 29.10.2022 r.
3. https://www.iustitia.pl/dzialalnosc/opinie-i-raporty/4318-raport-iustitii-o-statystykach-wymiaru-sprawiedliwosci z dnia 29.10.2022 r.
4. https://www.currentware.com/blog/internet-usage-statistics/ z dnia 27.10.2022 r.
5. https://pl.wikipedia.org/wiki/Telekomunikacja z dnia 29.10.2022 r.
6. https://pl.wikipedia.org/wiki/Payment_Services_Directive z dnia. 27.10.2022 r.
7. https://www.websiterating.com/pl/research/internet-statistics-facts/#chapter-1 z dnia 27.10.2022 r.
8. https://www.nask.pl/ z dnia 27.10.2022 r.
9. https://www.nask.pl/ z dnia 27.10.2022 r.
10. https://encyklopedia.pwn.pl/haslo/nizaryci;3947980.html z dnia 29.10.2022 r.
11. https://pl.wikipedia.org/wiki/Al-Ka%E2%80%99ida z dnia 29.10.2022 r.
12. https://www.nask.pl/pl/aktualnosci/4266,CERT-Polska-informuje-o-znacznym-wzroscie-liczby-oszustw-komputerowych.html z dnia 20.06.2022 r.
13. Wikipedia, https://pl.wikipedia.org/wiki/WikiLeaks, z dnia 27.06.2022 r.
14. Statista, https://www.statista.com/statistics/1028557/poland-cybersecurity-incidents/
15. z dnia 28.06.2022 r.
16. https://www.gov.pl/web/baza-wiedzy z dnia 17.10.2022 r.
17. https://www.gov.pl/web/mswia/powstanie-centralne-biuro-zwalczania-cyberprzestepczosci z dnia 20.10.2022 r.
18. https://www.nask.pl/, z dnia 21.10.2022 r.
19. https://cert.pl/o-nas/ z dnia 21.10.2022 r.
20. https://www.statista.com/statistics/266155/number-of-phishing-domain-names-worldwide/ z dnia 27.10.2022 r.
21. https://financesonline.com/how-much-data-is-created-every-day/ z dnia 22.10.2022 r.
22. https://it-szkola.edu.pl/ z dnia 27.10.2022 r.
23. https://niebezpiecznik.pl/ z dnia. 27.10.2022 r.

24. https://zaufanatrzeciastrona.pl/ z dnia 27.10.2022 r.
25. http://www.zrozumiecpolske.pl/rodzaje-socjotechnik/ z dnia 28.10.2022 r.
26. https://www.corazlepszafirma.pl/blog/bezpieczenstwo-danych-firmy
z dnia 28.10.2022 r.
27. https://pl.wikipedia.org/wiki/Robak_Morrisa z dnia 28.10.2022 r.
28. https://en.wikipedia.org/wiki/Blue_Frog z dnia 28.10.2022 r.
29. https://pl.wikipedia.org/wiki/Terror z dnia 29.10.2022 r.
30. https://pl.wikipedia.org/wiki/WannaCry z dnia 29.11.2022 r.
31. https://en.wikipedia.org/wiki/Titan_Rain z dnia 29.10.2022 r.
32. en.wikipedia.org/wiki/Timeline_of_events_associated_with_Anonymous
z dnia 29.10.2022 r.
33. https://en.wikipedia.org/wiki/Common_Vulnerability_Scoring_System
z dnia 29.10.2022 r.
34. https://javaheri.pl/co-to-jest-cve-i-czemu-warto-zglaszac-podatnosci/
z dnia 29.10.2022 r.
35. https://whitehats.pwr.edu.pl/research/podatnosci-wstep/ z dnia 29.10.2022 r.
36. https://www.oracle.com/pl/artificial-intelligence/what-is-ai/ z dnia 29.10.2022 r.
37. Dane z Komendy Głównej Policji, z wykazu Krajowego Systemu Informacji Policji z zakresu lat 2016-2022, Warszawa z dnia 21.04.2022 r.
38. Informacje uzyskane od Policjantów w drodze doświadczeń własnych z atakami phishingowymi

Wykaz Ilustracji

Wykaz tabel

Wykaz wykresów