Wstęp

Ryzyko przestępczości komputerowej stało się problemem globalnym, dotykającym prawie wszystkie kraje. Internet jest „mieczem obosiecznym", który daje wiele możliwości rozwoju i prosperowania jednostek i organizacji, ale jednocześnie niesie ze sobą nowe możliwości popełniania przestępstw. Na przykład przestępczość finansowa związana z Nigerią jest szeroko rozpowszechniona, a 122 ze 138 krajów na spotkaniu Interpolu skarżyło się na udział Nigerii w oszustwach finansowych w ich krajach. Najbardziej znanym rodzajem ataków na pracowników biurowych na całym świecie jest tak zwane oszustwo z zaliczką. Nadawca będzie starał się zaangażować odbiorcę w plan zarobienia milionów dolarów, jeśli odbiorca zapłaci zaliczkę. Przestępczość komputerowa to przytłaczający problem na całym świecie. Przyniósł szereg nowych działań i aktorów rymowych, a w konsekwencji szereg nowych wyzwań w walce z tym nowym zagrożeniem Kontrolowanie przestępczości komputerowej jest rzeczywiście wyzwaniem wymagającym dużej wiedzy ze względu na innowacyjny aspekt wielu rodzajów przestępczości komputerowej. Cyberprzestrzeń stanowi nowe wyzwanie dla kryminologii, nauki o policji, organów ścigania i policji. Rzeczywistość wirtualna i komunikacja za pośrednictwem komputera stanowią wyzwanie dla tradycyjnego dyskursu kryminologii i pracy policji, wprowadzając nowe formy dewiacji, przestępczości i kontroli społecznej. Od lat 90. naukowcy i praktycy obserwowali, jak cyberprzestrzeń pojawiła się jako nowa dziedzina działalności przestępczej. Cyberprzestrzeń zmienia charakter i zakres przestępstw i wiktymizacji. Pojawia się nowa dyscyplina o nazwie cyberkryminologia. Jaishankar definiuje cyberkryminologię jako badanie przyczyn przestępstw występujących w cyberprzestrzeni i ich wpływu na przestrzeń fizyczną.

Definicja cyberprzestępczości

Pracownicy organizacji popełniają większość przestępstw komputerowych, a przestępstwo to odbywa się wewnątrz murów firmy. Jednak w naszej perspektywie przestępczości finansowej przedstawionej tu zdefiniujemy przestępczość komputerową jako przestępstwo nastawione na zysk, a nie przestępstwo nastawione na szkodę, wykluczając w ten sposób tradycyjne skupienie się na niezadowolonych i sfrustrowanych pracownikach, którzy chcą zaszkodzić własnym pracodawcom.

Technologia przestępczości komputerowej

Przestępczość komputerowa jest definiowana jako wszelkie naruszenia prawa karnego, które wiążą się ze znajomością technologii komputerowej w celu ich popełnienia, dochodzenia lub ścigania. Początkową rolą technologii informacyjno-komunikacyjnych była poprawa wydajności i efektywności organizacji. Jednak dążenie do wydajności i skuteczności służy bardziej niejasnym celom, ponieważ oszuści wykorzystują wymiar elektroniczny do osobistych korzyści. Przestępczość komputerowa to przytłaczający problem, który przyniósł szereg nowych rodzajów przestępstw. Przykłady przestępstw komputerowych obejmują sabotaż, piractwo komputerowe i kradzież danych osobowych . W terminologii przestępczości komputerowej termin cracker jest zwykle używany do określenia hakera z zamiarem przestępczym. Nikt nie zna skali problemu przestępczości komputerowej – ile systemów zostało zaatakowanych, ile osób angażuje się w tę praktykę, czy też całkowite szkody ekonomiczne. Według Laudona i Laudona najbardziej szkodliwymi ekonomicznie rodzajami przestępstw komputerowych są ataki typu „odmowa usługi", w ramach których zamówienia klientów mogą być przekierowywane do innego dostawcy. Jedenastu mężczyzn w pięciu krajach dokonało jednej z najgorszych kradzieży danych dotyczących oszustw związanych z kartami kredytowymi: Na początku sierpnia 2008 r. amerykańscy prokuratorzy federalni oskarżyli 11 mężczyzn w pięciu krajach, w tym w Stanach Zjednoczonych, Ukrainie i Chinach, o kradzież ponad 41 milionów numerów kart kredytowych i debetowych. Jest to obecnie największa znana kradzież numerów kart kredytowych w historii.

Złodzieje skupili się na głównych sieciach handlowych, takich jak OfficeMax, Barnes & Noble, BJ's Wholesale Club, Sports Authority i T.J. Marksa.

Złodzieje jeździli i skanowali sieci bezprzewodowe tych sprzedawców w celu zidentyfikowania luk w zabezpieczeniach, a następnie zainstalowali programy sniffer uzyskane od zagranicznych współpracowników. Programy sniffer podsłuchiwały sieci sprzedawców detalicznych w celu przetwarzania kart kredytowych, przechwytując numery kart debetowych i kredytowych oraz PIN-y (osobiste numery identyfikacyjne). Złodzieje wysłali te informacje do komputerów na Ukrainie, Łotwie i w Stanach Zjednoczonych. Sprzedawali numery kart kredytowych przez Internet, a inne skradzione numery umieszczali na paskach magnetycznych pustych kart, aby móc wypłacić tysiące dolarów z bankomatów. Albert Gonzales z Miami został zidentyfikowany jako główny organizator ringu.

Spiskowcy rozpoczęli swoją największą kradzież w lipcu 2005 roku, kiedy zidentyfikowali zagrożoną sieć w domu towarowym Marshalla w Miami i użyli jej do zainstalowania programu sniffer na komputerach firmy macierzystej sieci, TJX. Udało im się uzyskać dostęp do centralnej bazy danych TJX, w której przechowywano transakcje klientów dla T.J. Marxx, Marshalls, HomeGoods i A.J. Sklepy Wright w Stanach Zjednoczonych i Portoryko oraz sklepy Winners i HomeSense w Kanadzie. Piętnaście miesięcy później TJX poinformował, że intruzi ukradli rekordy zawierające do 45 milionów numerów kart kredytowych i debetowych.

TJX nadal używał starego systemu szyfrowania Wired Equivalent Privacy (WEP), który jest stosunkowo łatwy do złamania przez hakerów. Inne firmy przeszły na bezpieczniejszy standard Wi-Fi Protected Access (WPA) z bardziej złożonym szyfrowaniem, ale TJX nie wprowadził zmiany. Audytor stwierdził później, że TJX zaniedbał również instalację zapór ogniowych i szyfrowania danych na wielu komputerach korzystających z sieci bezprzewodowej, a także nie zainstalował poprawnie kolejnej warstwy oprogramowania zabezpieczającego, które zakupiła. TJX przyznał w Komisji Papierów Wartościowych i Giełd, że przesyła dane kart kredytowych do banków bez szyfrowania, naruszając wytyczne firmy obsługującej karty kredytowe.

Przestępczość komputerowa, często używana jako synonim cyberprzestępczości, odnosi się do każdego przestępstwa, które dotyczy komputera i sieci, w których komputer odegrał rolę w popełnieniu przestępstwa. Przestępczość internetowa, jako trzecia etykieta przestępczości, odnosi się do przestępczego wykorzystywania Internetu. Z naszej perspektywy przestępczości nastawionej na zysk, przestępczość jest ułatwiana przez sieci lub urządzenia komputerowe, w których głównym celem nie są sieci i urządzenia komputerowe, ale raczej niezależne od sieci lub urządzenia komputerowego.

Przestępczość komputerowa w Internecie

Cyberprzestępczość to termin używany do ataków na infrastrukturę cyberbezpieczeństwa organizacji biznesowych, które mogą mieć kilka celów. Jednym z celów przestępców jest uzyskanie nieautoryzowanego dostępu do poufnych informacji celu. Większość firm jest w dużym stopniu uzależniona od informacji zastrzeżonych, w tym informacji o nowych produktach, danych o zatrudnieniu, cenników i danych dotyczących sprzedaży. Według Gallahera napastnik może czerpać bezpośrednie korzyści ekonomiczne z uzyskania dostępu do takich informacji i/lub ich sprzedaży lub może wyrządzić szkodę organizacji, wpływając na nią. Po uzyskaniu dostępu osoby atakujące mogą nie tylko wydobywać i wykorzystywać lub sprzedawać informacje poufne, ale także modyfikować lub usuwać informacje poufne, co ma poważne konsekwencje dla ich celów. Cyberprzestępczość to każde przestępstwo popełnione za pośrednictwem sieci komputerowej. Cyberprzestępczość nie ogranicza się do ataków z zewnątrz. Według Nykodyma najczęstszy rodzaj cyberprzestępców ma miejsce w ich własnych murach. Jednak większość tych rodzajów przestępstw jest niewinna i małostkowa. Przykłady obejmują czytanie gazet online, śledzenie wydarzeń sportowych w pracy lub hazard online. Większość

sprawców ma od 30 do 35 lat. Niektóre rodzaje przestępstw są poważne, na przykład kradzież. Najwięcej szkód wyrządzają osoby powyżej 35 roku życia. Zarówno cyberprzestępczość, jak i przestępczość komputerowa są powiązane z przestępczością internetową. Internet to „miecz obosieczny", który daje wiele możliwości rozwoju osobom i organizacjom. Jednocześnie Internet przyniósł ze sobą nowe możliwości popełniania przestępstw. Salifu przekonuje, że przestępczość internetowa stała się problemem globalnym, który wymaga pełnej współpracy i udziału zarówno krajów rozwijających się, jak i rozwiniętych na szczeblu międzynarodowym. Oszustwo związane z kliknięciami ma miejsce, gdy osoba fizyczna lub program komputerowy nieuczciwie klika reklamę online bez zamiaru uzyskania dodatkowych informacji o reklamodawcy lub dokonania zakupu. Kiedy klikniesz w reklamę wyświetlaną przez wyszukiwarkę, reklamodawca zazwyczaj uiszcza opłatę za każde kliknięcie, które ma na celu skierowanie potencjalnych nabywców do jego produktu. Oszustwa związane z kliknięciami stały się poważnym problemem w Google i innych witrynach internetowych oferujących reklamy online typu „płatność za kliknięcie". Niektóre firmy zatrudniają strony trzecie (zwykle z krajów o niskich płacach) do nieuczciwego klikania reklam konkurencji w celu ich osłabienia poprzez zwiększenie kosztów marketingu. Oszustwa związane z kliknięciami mogą być również popełniane przez programy wykonujące kliknięcia

Finansowe przestępstwa komputerowe

U nas przestępczość komputerowa jest klasyfikowana jako przestępstwo finansowe. Przestępstwo finansowe można zdefiniować jako przestępstwo przeciwko mieniu, polegające na bezprawnym przekształceniu cudzego mienia na własny użytek i korzyść. Przestępstwa finansowe są czasami określane mianem przestępstw gospodarczych. Przestępczość finansowa to przestępstwo nastawione na zysk, mające na celu uzyskanie dostępu do mienia, które należało do kogoś innego i kontrolę nad nim. Pickett i Pickett definiują przestępstwo finansowe jako wykorzystanie oszustwa w celu uzyskania nielegalnych korzyści, zwykle wiążące się z naruszeniem zaufania i zatajeniem prawdziwego charakteru tych działań. Używają zamiennie terminów przestępstwo finansowe, przestępstwo białych kołnierzyków i oszustwo. Termin przestępstwo finansowe wyraża różne koncepcje w zależności od jurysdykcji i kontekstu. Niemniej jednak Henning twierdzi, że przestępczość finansowa ogólnie opisuje różne przestępstwa przeciwko mieniu, obejmujące bezprawne przekształcenie mienia należącego do innej osoby na własny użytek i korzyść, najczęściej obejmujące oszustwo, ale także przekupstwo, korupcję, pranie pieniędzy, sprzeniewierzenie, handel poufny, naruszenia podatkowe, cyberataki i tym podobne. Wydaje się, że jedną z podstawowych cech przestępczości finansowej jest zysk z przestępstwa dla korzyści osobistych. Przestępczość finansowa często wiąże się z oszustwem. Przestępstwa finansowe są dokonywane za pomocą oszustw związanych z czekiem i kartami kredytowymi, oszustwami hipotecznymi, oszustwami medycznymi, oszustwami korporacyjnymi, oszustwami na kontach bankowych, oszustwami dotyczącymi płatności (punktów sprzedaży), oszustwami walutowymi i oszustwami dotyczącymi opieki zdrowotnej, i obejmują takie działania, jak wykorzystywanie informacji poufnych, naruszenia podatków, łapówki, defraudacje, kradzież tożsamości, cyberataki, pranie brudnych pieniędzy i socjotechnika. Defraudacja i kradzież mienia związkowego oraz fałszowanie rejestrów związkowych wykorzystywane do ułatwiania lub ukrywania takich kradzieży pozostają najczęściej ściganymi w USA przestępstwami na podstawie Ustawy o raportowaniu i ujawnianiu informacji o zarządzaniu pracownikami. Przestępstwa finansowe czasami, ale nie zawsze, obejmują czyny przestępcze, takie jak znęcanie się nad osobami starszymi, napady z bronią w ręku, włamania, a nawet morderstwa. Ofiary obejmują różne osoby, instytucje, korporacje, rządy i całe gospodarki. Interpol twierdzi, że przestępstwa finansowe i zaawansowane technologicznie - na przykład fałszowanie pieniędzy, pranie pieniędzy, przestępstwa przeciwko własności intelektualnej, oszustwa związane z kartami płatniczymi, ataki wirusów komputerowych i

cyberterroryzm – mogą mieć wpływ na wszystkie poziomy społeczeństwa. Znajdujemy wiele różnych działań przestępczych, które można zaklasyfikować jako przestępstwa finansowe.

PRZESTĘPSTWO FINANSOWE

Korupcja :

Łapówkarstwo

Odbicia

Organizacja

Publiczny

Oszustwo :

Opłata zaliczkowa

Bank

Sprawdź

Kliknij

Konsument

Karta kredytowa

Sprzeniewierzenie

Fundusz hedgingowy

Tożsamość

Hipoteka

Zawód

Subsydium

Kradzież :

Sztuka

Tożsamość

Gotówka

Intelekt

Spis

Manipulacja :

Bankructwo

Oferta

Komputer

Konkurencja

Cyber

Waluta

Faktura

Wymuszenie

Duch

Pranie

Podatek

Cztery główne kategorie to odpowiednio korupcja, oszustwo, kradzież i manipulacja. W ramach każdej głównej kategorii istnieje szereg podkategorii. Przestępczość komputerowa została sklasyfikowana jako podkategoria manipulacji jako główna kategoria. Manipulację można zdefiniować jako sposób uzyskania nielegalnej kontroli lub wpływu na działania, środki i wyniki innych osób. Oprócz tego bezpośredniego rodzaju przestępczości komputerowej, spotykamy pośrednie formy przestępczości komputerowej, w których istotnym elementem przestępstwa jest technologia komputerowa. Wspomnieliśmy już o przykładach takich jak oszustwa tożsamości; oszustwa kliknięcia i oszustwa związane z kartami kredytowymi, które można znaleźć w głównej kategorii oszustw. Definiując przestępstwa komputerowe jako przestępstwa finansowe, a czasem nawet jako przestępstwa białych kołnierzyków, jak omówiono poniżej, skupiamy się na zorientowaniu na zysk takich przestępczość. Definicja ta wyklucza przestępstwa komputerowe mające na celu wyrządzenie szkody bez zysku. Nawet jeśli infekcja złośliwym oprogramowaniem, hakowanie i inne incydenty są często zgłaszane w prasie popularnej, tego rodzaju przestępstwa komputerowe są tutaj interesujące tylko wtedy, gdy mają motywację zarobkową. Przestępczość komputerowa jest tutaj przestępstwem nastawionym na zysk, mającym na celu uzyskanie dostępu do własności, która należała do kogoś innego i kontrolę nad nią. Przestępczość zarobkową popełnianą przez przestępców należy rozumieć głównie w kategoriach ekonomicznych, a nie socjologicznych czy kryminologicznych. Próbując sformułować ogólną teorię przestępczości nastawionej na zysk, Naylor zaproponował typologię, która przenosi punkt ciężkości z aktorów na działania, rozróżniając przestępczość rynkową, drapieżną i handlową. Teoria przestępczości motywowanej zyskiem w przypadku przestępczości białych kołnierzyków sugeruje, że przestępstwa finansowe są motywowane możliwościami, w przypadku których kierownictwo i menedżerowie identyfikują możliwości nielegalnego zysku. Szansa jest elastyczną cechą przestępstwa finansowego i różni się w zależności od rodzaju zaangażowanych przestępców

Przestępczość komputerowa związana z białymi kołnierzykami

Przestępczość komputerowa może występować w ramach przestępczości białych kołnierzyków, która jest szczególną dziedziną przestępczości finansowej. Przestępczość białych kołnierzyków można zdefiniować w kategoriach przestępstwa, sprawcy lub obu. Jeśli przestępstwo białych kołnierzyków jest definiowane jako przestępstwo, oznacza to przestępstwo przeciwko mieniu w celu osiągnięcia korzyści osobistej lub organizacyjnej. Jest to przestępstwo przeciwko mieniu popełnione przy użyciu środków niefizycznych oraz poprzez ukrycie lub oszustwo. Jeśli przestępstwo białych kołnierzyków definiuje się

w kategoriach sprawcy, oznacza to przestępstwo popełnione przez członków wyższej klasy społeczeństwa dla osobistych lub organizacyjnych korzyści. To osoby zamożne, dobrze wykształcone i powiązane społecznie, które są zazwyczaj zatrudnione przez legalne organizacje i w nich. Jeśli przestępczość białych kołnierzyków jest definiowana z obu perspektyw, przestępczość białych kołnierzyków ma następujące cechy:

• Przestępczość białych kołnierzyków to przestępstwo przeciwko mieniu w celu uzyskania korzyści osobistych lub organizacyjnych, które jest popełniane w sposób niefizyczny oraz poprzez ukrycie lub oszustwo. Jest zwodnicza, celowa, podważa zaufanie i pociąga za sobą straty.

• Przestępcy „białych kołnierzyków" to osoby zamożne, dobrze wykształcone i powiązane społecznie, zazwyczaj zatrudnione przez legalną organizację. Są to osoby cieszące się szacunkiem i wysokim statusem społecznym, które popełniają przestępstwo w trakcie wykonywania zawodu.

Nie tylko najbardziej pokrzywdzeni ekonomicznie członkowie społeczeństwa popełniają przestępstwa. Członkowie uprzywilejowanej klasy społeczno-ekonomicznej są również zaangażowani w zachowania przestępcze. Rodzaje przestępstw mogą różnić się od tych z niższych klas, takich jak prawnicy pomagający klientom przestępczym w praniu pieniędzy, kierownictwo przekupujące urzędników publicznych w celu uzyskania zamówień publicznych lub księgowi manipulujący bilansami w celu uniknięcia podatków. Inną ważną różnicą między tymi dwoma sprawcami jest to, że elitarny przestępca jest znacznie mniej narażony na zatrzymanie lub ukaranie ze względu na jego status społeczny. Edwin Sutherland wprowadził koncepcję przestępczości „białych kołnierzyków" w 1939 roku. Według Brightmana teoria Sutherlanda była kontrowersyjna, zwłaszcza że wielu akademików na widowni uważało się za członków wyższej warstwy amerykańskiego społeczeństwa. Pomimo jego krytyków, teoria Sutherlanda dotycząca przestępczości białych kołnierzyków posłużyła jako katalizator dla obszaru badań, które trwają do dziś. W przeciwieństwie do Sutherlanda Brightman różni się nieco w kwestii definicji przestępczości białych kołnierzyków. Chociaż status społeczny może nadal determinować dostęp do bogactwa i własności, twierdzi on, że termin „przestępczość białych kołnierzyków" powinien mieć szerszy zakres i obejmować praktycznie każdy akt pokojowy popełniony w celu uzyskania korzyści finansowych, niezależnie od statusu społecznego. Na przykład dostęp do technologii, takich jak komputery osobiste i Internet, pozwala teraz jednostkom ze wszystkich klas społecznych kupować i sprzedawać akcje lub angażować się w podobne działania, które kiedyś były bastionem elity finansowej. Salifu wspiera naszą perspektywę przestępczości komputerowej jako przestępstwa nastawionego na zysk, przestępstwa finansowego, a czasem nawet przestępczości białych kołnierzyków, argumentując, że podstawą przestępczości internetowej jest rozum ekonomiczny. Chociaż może istnieć wiele motywów, takich jak władza, żądza, zemsta, przygoda i chęć sprawdzenia nielegalnych granic oraz prawdopodobieństwo złapania, najbardziej oczywistym motywem jest chciwość i zysk. O wiele więcej przestępstw komputerowych jest motywowanych chciwością i perspektywą korzyści finansowych niż jakikolwiek inny motyw. Przestępczość białych kołnierzyków stanowi poważne zagrożenie dla reputacji firmy. Niemniej jednak istnieje zaskakująco wiele korporacji zaangażowanych w przestępczość białych kołnierzyków. Na przykład w Szwecji Alalehto odkrył, że 40 procent czołowych korporacji w szwedzkim świecie biznesu było zamieszanych w przestępczość w białych kołnierzykach w ciągu ostatniej dekady. Korporacje te miały przeciwko nim decyzje, takie jak orzeczenia sądowe, prawo administracyjne, sprzeciw czy ugoda.

Sprawca lub ofiara przestępstwa

Większość badań wydaje się uwzględniać perspektywę ofiar przestępstw komputerowych. Z tej perspektywy wynika, że ofiarą przestępstwa jest jednostka, grupa, organizacja lub społeczeństwo. Tutaj również zastosujemy perspektywę sprawcy. Perspektywa przestępcy sugeruje, że osoba, grupa,

organizacja lub społeczeństwo jest przestępcą odpowiedzialnym za przestępstwo komputerowe. Z perspektywy ofiar badanie wykazało, że obok infekcji złośliwym oprogramowaniem i kradzieży sprzętu IT najczęściej zgłaszanym incydentem przestępstwa komputerowego był haker. Ustalenia Hagena dowodzą, że przestępczość komputerowa powoduje dodatkową pracę dla ofiary, a także utratę zarobków. Kilku zgłoszonym w ich badaniu incydentom przestępczym można by przeciwdziałać dzięki lepszej kontroli dostępu i środkom ochrony danych, a także działaniom uświadamiającym. Ankieta wykazała, że istnieją duże różnice w praktykach bezpieczeństwa między dużymi i małymi przedsiębiorstwami, nawet jeśli chodzi o środki, które można by pomyśleć, że zostałyby wdrożone wszystkie przedsiębiorstwa niezależnie od wielkości.