Prokuratura Görlitz

Cyberprzestępczość, zjawisko bez granic

1. Wprowadzenie

Pojęcie przestępczości komputerowej lub cyberprzestępczości (ang. Cybercrime) obejmuje wszystkie czyny karalne, które są popełniane z wykorzystaniem technik teleinformatycznych (ITC) lub przeciw nim. Jest to szeroka dziedzina. Dlatego chciałbym się w tym opracowaniu zająć cyberprzestępczością w ścisłym znaczeniu tego słowa. Prokuratura Generalna Wolnego Państwa Saksonia definiuje ją następująco:

a) czyny karalne szczególne, podczas których elementy elektronicznego przetwarzania danych są zawarte w znamionach czynu przestępczego. Dotyczy to również czynów karalnych wg §§ 202a, 202b, 202c, 263a, 269, 270, 271, 274 ust. 1 nr 2 i ust 2, oraz §§ 303a, 303b, 348 niemieckiego Kodeksu Karnego (StGB), § 17 ust. 2 nr 1 litera a i nr 2 Ustawy o nieuczciwej konkurencji (UWG), §§ 106 do 108b Ustawy o ochronie praw autorskich (UrhG) i § 44 w połączeniu z § 43 Federalnej Ustawy o ochronie danych (BDSG) – a więc np. bezprawnego wejścia w posiadanie danych komputerowych, oszustw komputerowych, fałszowania danych dowodowych, sabotażu komputerowego, i innych;

b) przestępstwa powszechne, przy popełnianiu których zastosowano techniki teleinformatyczne w sieciach danych, zwłaszcza w celu zatajenia tożsamości sprawców, a dla przeprowadzenia dowodu jest wymagany wysoki stopień wiedzy technicznej. Uzasadnieniem wysokiego stopnia wiedzy technicznej jest już samo to, że dla ustalenia tożsamości sprawców jest konieczne ustalenie danych stałych lub adresu IP.

2. Statystyka

Niestety do dyspozycji miałem tylko dane z 2015 roku. Z powodu zmian metod ewidencji liczba zdarzeń wynosząca 45.793 czynów karalnych spadła o 8,3 % w stosunku do 2014 roku. Tym niemniej suma całkowita szkód wzrosła o 2,8 % w stosunku do roku poprzedniego i wyniosła 40,5 mln. EUR, przy czym dotyczy to tylko grupy czynów oszustw komputerowych i oszustw w związku prawami dostępu do usług komunikacyjnych, ponieważ tylko w tych grupach czynów prowadzi się ewidencję szkód. Wskaźnik wykrywalności wzrósł o 3,4 % do 32,8 %.

3. Najczęstsze znamiona przestępstwa

a) oszustwo komputerowe (§ 263a StGB (niem. kk)) obejmuje zwłaszcza działanie z wykorzystaniem Phishing-u (przykład: Inicjalizację bezprawnych transakcji w bankowości elektronicznej z wykorzystaniem złośliwego oprogramowania), transakcje z wykorzystaniem bezprawnie pozyskanych danych kart kredytowych i z zastosowaniem skradzionych lub sfałszowanych kart płatniczych w bankomatach lub terminalach płatniczych.

b) oszustwo w związku z prawami dostępu do usług komunikacyjnych (częsta forma szczególna § 263a StGB) oznacza manipulację urządzeń telekomunikacyjnych przy wykorzystaniu luk w zabezpieczeniach lub słabych zabezpieczeń dostępu zarówno w firmach jak i w prywatnych gospodarstwach domowych (np. przez nieuprawniony dostęp do routera

wybierane są drogie połączenia telefoniczne z zagranicą lub specjalnie korzysta się z usług typu premium wzgl. z usług dodanych.)

c) bezprawne wejścia w posiadanie i przechwytywanie danych (§§ 202a, 202b StGB) obejmuje „kradzież" tożsamości cyfrowej, danych kart kredytowych, kart do handlu internetowego lud danych kont (np. phishing). Skradzione dane są z reguły oferowane jako towar handlowy na internetowym czarnym rynku lub bezprawnie wykorzystywane przez sprawców. Wykorzystanie odbywa się tym samym w dwóch fazach, sprzedaży danych i oszukańczym zastosowaniu pozyskanych danych. Na obu płaszczyznach uzyskuje się znaczne zyski.

d) fałszowanie danych o znaczeniu dowodowym (§ 269 StGB) obejmuje wprowadzenie w błąd (osoby) przez fałszowanie danych. Posiadacz danych fałszuje wzgl. podrabia dane i stosuje je do wprowadzania w błąd w obrocie prawnym. To dzieje się np. poprzez wysyłanie e-mail-i udawanie realnej tożsamości lub firm. Przekonującymi legendami ofiara ma być nakłoniona np. do zdradzenia informacji o koncie, danych kart kredytowych lub też do płatności. Obejmuje także przysyłanie złośliwego oprogramowania zamaskowanego jako rachunki w załącznikach poczty elektronicznej.

e) Modyfikacja danych / sabotaż komputerowy (§§ 303a, 303b StGB) obejmuje modyfikację danych w systemie przetwarzania danych wzgl. modyfikację systemu przez innych niż posiadacz danych np. przez ataki Denial of Service (ataki DoS są wymierzone przeciwko dostępności usług, stron internetowych, pojedynczych systemów lub całych sieci. Jeżeli atak jest przeprowadzany za pomocą wielu systemów równolegle, wtedy mówi się o dzielonym ataku DoS lub o ataku DDoS (DDoS = Distributed Denial of Service, ataki DDoS odbywają się często na dużej liczbie komputerów lub serwerów).
Pod to podchodzi także rozpowszechnianie i stosowanie złośliwego oprogramowania różnego rodzaju (koni trojańskich, wirusów, robaków itd.).

4. Częste formy popełniania

a) Szantaż internetowy z zastosowaniem tzw. oprogramowania typu ransomware

Ransomware to złośliwe oprogramowanie, za pomocą którego natręt powoduje uniemożliwienie dostępu lub korzystania z poszczególnych danych lub z całego systemu komputerowego. Za (rzekome) zwolnienie systemu informatycznego lub danych żąda się okupu (po angielsku: ransom). Odpowiednie złośliwe oprogramowanie lub też całą „usługę" (np w tzw. modelu partnerskim „model affiliate") można nabyć np. na forach podziemia gospodarczego w darknecie, i dlatego obecnie nie jest wymagana szczególna wiedza z dziedziny IT do przeprowadzenia cyfrowego szantażu. Affiliate opisuje stosunek między producentem oprogramowania typu ransomware a kupującym, który odbiera je jako usługę. Producent oferuje pewne wsparcie (jak update-y, konserwację, korzystanie z serwerów). Konkretne rozpowszechnianie oprogramowania typu ransomware jest zadaniem klienta. Oferenci usługi otrzymują po zapłacie okupu pewien udział w obrocie, przy czym zapłata okupu jest realizowana w formie wirtualnej waluty „bitcoin" przez samego oferenta złośliwego oprogramowania. Poprzez platformę kontrolną użytkownik oprogramowania typu ransomware może sam sobie wypłacić udział w okupie. Istnieją 2 warianty oprogramowania

typu ransomware. Prosty wariant zabrania przez manipulację jedynie dostępu do systemu w sensie blokady. Natomiast tzw. oprogramowanie krypto-ransomware jest znacznie bardziej niebezpieczne, ponieważ faktycznie szyfruje dane w zainfekowanych systemach.
Wiele osób płaci żądany okup, bo wśród poszkodowanych istnieje bardzo duża presja, żeby odzyskać swoje dane. Według ankiety pewnego oferenta oprogramowania zabezpieczającego 33 % poszkodowanych w Niemczech przez oprogramowanie typu ransomware zapłaciło okup a 36 % użytkowników Internetu w Niemczech jest zasadniczo gotowe spełnić żądania szantażystów. Gotowość zapłaty w Niemczech to kwota średnio 211 Euro. Od grudnia 2015 roku notuje się wielki zalew spamu, przez który masowo rozpowszechnia się ransomware. W ponad 95 % chodzi o ransomware z funkcjami szyfrowania.

b) usługi typu „Cybercrime-as-a-Service“

Pod tym pojęciem rozumie się udostępnianie oprogramowania i usług do popełniania czynów karalnych. Oferta nielegalnych usług tego rodzaju obejmuje np.:

• ransomware (i jego pakiety narzędziowe)
• udostępnianie botnetów dla działalności kryminalnej,
• ataki typu DDoS,
• produkcję i rozpowszechnianie malware-u,
• kradzież danych,
• sprzedaż / oferowanie wrażliwych danych, np. danych dostępowych lub płatniczych,
• pośrednictwo agentów finansowych i towarowych, którzy za opłatą tuszują pochodzenie środków finansowych lub towarów uzyskanych w wyniku czynów karalnych,
• platformy komunikacyjne do wymiany kryminalnej wiedzy, jak na przykład fora podziemia gospodarczego,
• usługi anonimizacji i usługi hostingowe do tuszowania własnej tożsamości,
• tzw. dropzones do przechowywania nielegalnie uzyskanych informacji i / lub towarów.

To wszystko umożliwia przeprowadzanie cyberataków także przestępcom nie posiadającym wiedzy technicznej i stosunkowo małym kosztem.

Te usługi są oferowane przez „darknet“ na nielegalnych forach lub rynkach internetowego podziemia gospodarczego. Fora służą także do komunikowania się cyberprzestępców i do transferu wiedzy kryminalnej. Oferenci tych usług podlegają karze na podstawie §§ 202c, 263a ust. 3 kk (StGB) albo przynajmniej za podżeganie lub pomocnictwo w czynach popełnianych bezpośrednio przez sprawców.

Ponadto w "darknecie" realizuje się wszelkie rodzaje nielegalnych transakcji, i tak w Lipsku pewien młody mężczyzna prowadził w darknecie kwitnący handel narkotykami czy szaleniec z Monachium kupił przez darknet broń.

c) kradzież tożsamości cyfrowej i nadużycie tożsamości

Pojęcie „tożsamości cyfrowej“ oznacza sumę wszelkich możliwości i praw pojedynczego użytkownika oraz jego danych osobowych i działań w ramach Internetu. Należą do tego dane dostępowe w następujących obszarach:
• komunikacja (usługi mailowe i komunikatorowe),

• handel elektroniczny (bankowość elektroniczna, elektroniczny obrót akcjami, portale dystrybucyjne wszelkiego rodzaju działające w Internecie),
• informacje branżowe (np. o dostępie online do firmowych zasobów technicznych),
• administracja elektroniczna (np. elektroniczne deklaracje podatkowe),
• przetwarzanie w chmurze (udostępnianie pamięci danych lub oprogramowania, poprzez sieć).

Poza tym wszystkie inne informacje istotne dla płatności (zwłaszcza karty kredytowe z adresami płatności oraz dalszymi informacjami) są częścią tożsamości cyfrowej. Żeby wejść w posiadanie tych informacji, często stosuje się obok tzw. „konie trojańskie“ także inne metody z wykorzystaniem Internetu, jak np.:

• Instalację złośliwego oprogramowania przez Drive-by-exploits (podczas obserwowania strony internetowej, bez dalszych czynności użytkownika, są wykorzystywane słabe punkty w przeglądarce, we wtyczkach przeglądarki czy w systemie operacyjnym, żeby na komputerze niepostrzeżenie zainstalować konie trojańskie lub inne złośliwe oprogramowanie),
• Phishing (próby dostania się do danych osobowych użytkownika Internetu przez sfałszowane strony internetowe, e-maile czy SMS-y),
• włamania do serwerów i kopiowanie informacji logowania,
• zastosowanie keyloggerów (sprzętu lub oprogramowania do rejestracji naciskanych klawiszy i niezauważalnego przekazywania do agresora) lub programów szpiegujących (programy, które niepostrzeżenie zbierają dane o użytkowniku wzgl. o korzystaniu z komputera i przekazują do twórcy programu szpiegującego).

d) Phishing w bankowości elektronicznej

Wprawdzie w tym obszarze w 2015 roku spadła ilość przypadków w porównaniu z 2014 z 6.984 na 4.479 i tym samym o 35,9 %, ale i tak spowodował on szkody w wys. 17,9 mln EUR. Przyczyną spadku ma być wprowadzenie procedury TAN (inaczej niż w wypadku procedury iTAN z uprzednio sporządzoną ponumerowaną listą TAN dla każdego przelewu online jest generowany osobny numer transakcji i przekazywany klientowi sms-em). Sprawcy zareagowali na to z jednej strony tzw. manipulacją w czasie rzeczywistym. Do tego należą tzw. ataki typu "Man-In-the-Middle-" i "Man-In-the-Browser" (w przypadku ataku typu Man-In-The-Middle agresor wchodzi za pomocą trojana „do środka“ komunikacji, podając się wysyłającemu za odbiorcę a odbiorcy za wysyłającego , w przypadku ataków typu „Man-In-The-Browser“ oprogramowanie malware zainstalowane na komputerze manipuluje komunikację w ramach przeglądarki internetowej, przez co dalej przesyłane są inne informacje, niż te wprowadzane przez użytkownika). Prócz tego próbują za pomocą tzw. inżynierii społecznościowej dotrzeć do potrzebnych informacji o klientach. Znanym przykładem jest wysyłanie e-maili o charakterze budzącym zaufanie z żądaniem ujawnienia poufnych informacji z określonych przyczyn.

e) Niedozwolone użycie kart kredytowych za pomocą skimmingu.

"Skimming" oznacza "czerpanie" lub "spijanie śmietanki" i oznacza metodę nielegalnego kopiowania danych z karty płatniczej (karty debetowej i karty kredytowej). Żeby wejść w posiadanie danych z karty, sprawcy instalują przed czytnikiem kart w bankomatach lub w czytnikach kart w supermarketach zmanipulowany czytnik kart lub nawet całą płytę czołową. W ten sposób są zczytywane i zapisywane dane o koncie bez zakłócania obsługi

bankomatu wzgl. czytnika kart. Żeby zdobyć PIN, wybieranie numeru PIN jest rejestrowane ukrytą miniaturową kamerą. Tak uzyskane dane służą do wykonania kopii kart płatniczych. Przez to sprawcy mogą za (pozaeuropejską) granicą pobierać pieniądze z kont ofiar. Stosowanie fałszowania kart w niemieckich bankomatach jest niemożliwe z powodu tzw. "MM-Merkmal" (cecha modelowana; umieszczony w korpusie karty tajny kod maszynowy, który może być sprawdzany i porównywany przez niemieckie bankomaty) .

f) oszustwo przez sklepy typu fake

W przypadku sklepów typu fake sprawcy albo kopiują istniejący sklep internetowy wraz z jego ofertą towarów, albo tworzą własne sklepy najczęściej z drogimi towarami. Klienci często są kuszeni przez porównywarki cen ofertami znacznie tańszymi od oferty rynkowej. Zapłata za towar, który nigdy nie będzie dostarczony, odbywa się na konta założone na podstawie sfałszowanych danych osobowych albo na konta agentów finansowych, którzy te pieniądze przekazują zazwyczaj na konta zagraniczne lub na konta bitcoinowe

W takiej sprawie prokuratura w Görlitz prowadzi aktualnie dochodzenie. Przez taki fake-shop oferowano "korzystnie" drogie akcesoria basenowe. Płatność następowała na konto w banku Sparkasse Oberlausitz-Niederschlesien, założone na nazwisko czeskiego obywatela korzystającego z pomocy socjalnej, dyspozycje bankowe odbywały się zasadniczo przez Internet. Dochodzenie wykazało, że tenże obywatel korzystający z pomocy społecznej, który rzekomo miał być też operatorem sklepu, był wprawdzie obecny przy zakładaniu konta, jednakże wszelkie istotne aspekty zakładania konta były regulowane przez towarzyszącą mu nieznajomą osobę. Wpłaty były dalej przekazywane internetowo na konta zagraniczne lub bitcoinowe. Nie było wielu punktów zaczepienia dla wykrycia faktycznych sprawców. Obszerne ustalenie w ramach pomocy prawnej okazało się również bezowocne, ponieważ zagraniczne konta czy internetowe konta bitcoinowe z pewnością też zostały założone na fałszywe dane osobowe.

g) masowe zdalne sterowanie komputerami (botnety)

W botnetach wiele komputerów, zainfekowanych złośliwym kodem, jest bez wiedzy swoich właścicieli zdalnie sterowanych przez tzw. serwery Command & Control (serwery C&C). Instalacja złośliwego oprogramowanie na komputerach ofiar odbywa się w sposób niezauważalny dla właścicieli, np. przez otwarcie zainfekowanego załącznika poczty elektronicznej lub też przez „Drive-by-exploits“. Ostatnimi czasy nasila się rozpowszechnianie złośliwego oprogramowania przez sieci społecznościowe (np. Facebooka). Do uczestników sieci od przypuszczalnych znajomych lub przyjaciół (których tożsamość wzięto z komunikacji w Internecie) są rozsyłane wiadomości z zainfekowanymi załącznikami. Jeżeli te z powodu rzekomo istniejącej przyjaźni zostaną w dobrej wierze otwarte lub aktywują się linki, to komputer zostanie zainfekowany. Skutkiem tego sprawca przez zainstalowanie złośliwego oprogramowania ma niemal pełny dostęp do komputera ofiary. Kolejnym kanałem rozpowszechniania są Usenet (fora dyskusyjne) i giełdy wymiany / sieci P2P (Peer to Peer), w których złośliwe oprogramowanie jest ukryte w plikach wideo lub dźwiękowych oferowanych do ściągnięcia.

Botnety i ich możliwości stanowią ciągle jeszcze lukratywny towar handlowy na świecie w obszarze podziemia gospodarczego. Operatorzy botnetów wynajmują boty, poprzez które można przykładowo za pomocą ataków typu DDoS przeprowadzać celowane ataki na

serwery przedsiębiorstw, masowo rozsyłać spam w mailach czy też przeprowadzać celowane kradzieże danych.

h) Ataki typu DDoS na dostępność stron www, usług internetowych i sieci

Te ataki odbywają się z reguły przy użyciu komputera połączonego do botnetu. W samym pierwszym półroczu 2015 roku zarejestrowano 29.437 ataków typu DDoS . Właśnie w najbardziej konkurencyjnym segmencie rynku, jakim jest Internet, niemożność osiągnięcia portali dystrybucyjnych może prowadzić do znacznych szkód ekonomicznych. Dlatego ataki tego rodzaju są często połączone z próbami szantażu.

5. Rezultat

Cyberprzestępczość jest międzynarodowym zjawiskiem kryminalnym. Wynikający z niego potencjał zagrożenia i szkód ciągle rośnie. Wraz ze stale rosnącym znaczeniem informatyki w sferze prywatnej i zawodowej rosną możliwości manipulacji i ataków.

Dlatego w Wolnym Państwie Saksonia wdrożono celowane środki do zwalczania tego przestępczego zjawiska. We wszystkich prokuraturach są wyspecjalizowani prokuratorzy, którzy się zajmują zwalczaniem cyberprzestępczości. W moim wydziale jest dwóch prokuratorów dysponujących specjalistyczną wiedzą z dziedziny IT.

Ponadto w Wolnym Państwie Saksonia, zarówno w policji jak i w prokuraturach, coraz bardziej dąży się do zatrudniania śledczych, dysponujących pogłębioną wiedzą informatyczną. W prokuraturze w Görlitz taki śledczy ma być wkrótce zatrudniony.

Ostatnio w Prokuraturze Generalnej Wolnego Państwa Saksonia utworzono "Centralną Jednostkę Cybercrime Saksonia", której zadaniami są koordynacja współpracy z innymi krajami związkowymi oraz prokuraturami i jednostkami policji w Saksonii z jednej strony, i organizacja szkoleń i obserwacja nowych zjawisk z drugiej strony. Ma ona wspierać prokuratury w dochodzeniach i sporadycznie prowadzić własne dochodzenia w wyznaczonych przypadkach.