**Odcinek 20: „Kilka sposobów na włamywaczy i hakerów.”**

**Rafał Molenda:** Cały czas mam wrażenie, że ktoś nas podsłuchuje. Jeżeli tak jest, to bardzo dobrze, bo chyba na to trochę liczymy. Gorzej, gdy ten ktoś, kto nas podsłuchuje jeszcze nas podgląda. A jeszcze gorzej, kiedy ten ktoś oprócz tego, że nas podsłuchuje, podgląda to jeszcze wejdzie w posiadanie naszych danych wrażliwych.

To jest podcast Zachodniopomorskiego Uniwersytetu Technologicznego w Szczecinie.

O takich i podobnych sytuacjach będziemy rozmawiać dziś z Agnieszką Ubowską z Katedry Inżynierii Bezpieczeństwa i Energetyki na Wydziale Techniki Morskiej i Transportu Zachodniopomorskiego Uniwersytetu Technologicznego.

Dzień dobry.

**Agnieszka Ubowska:** Dzień dobry.

**Rafał Molenda:** Jak to jest z tym naszym bezpieczeństwem. Czy możemy się czuć bezpiecznie, żyjąc w tych okropnych czasach? To czasy, w których wszyscy się spieszą, mają aplikacje, mają swoje profile, różne konta w Internecie, kilkanaście haseł i loginów do różnych kont, korzystamy z samochodów, które łączą się z aplikacjami, i GPS i tych ścieżek dostępu do nas jest naprawdę bardzo dużo?

**Agnieszka Ubowska:** Tak dostępu do nas jest bardzo dużo, na szczęście nasze dane są chronione. Ochronę zapewnia ustawodawca. Daje nam to prawo do anonimowości. Daje nam to prawo do tego, żeby poszanować naszą prywatność. Tutaj przychodzi nam z pomocą technologia. Bywa też przeszkodą. Wspomniane przez Pana kilkanaście haseł to dobre rozwiązanie, dlatego że czasami zdarza się, że jedno hasło stosujemy wszędzie lub, że to hasło zawiera bardzo drobne modyfikacje. Takie zachowanie jest błędem. Należy od niego uciekać. Zdarza nam się chwalić różnymi informacjami. Mamy to w naturze, żeby informacje przekazywać. Dlaczego? Ot choćby z potrzeby podniesienia własnej wartości, chętnie chwalimy się znajomościami, wiedzą. Czasami chwalimy się tym, co dzieje się w pracy. Chwalimy tym, czym zajmuje się nasz pracodawca, czy dokąd zmierzają obrane przez niego drogi. Tego nie powinniśmy robić i musimy zdawać sobie z tego sprawę. Takie informacje zachowujemy dla siebie.

**Rafał Molenda:** To w takim razie mam usunąć wszystkie zdjęcia z Instagrama, wyłączyć Facebooka, jak żyć?

**Agnieszka Ubowska:** Był taki moment, że bardzo chciałam wyłączyć Facebooka, szczególnie po przeczytaniu książki Szamałka, który mówi o bezpieczeństwie w sieci.

Mechanizm jest przecież prosty, tracimy z kimś kontakt, a za sprawą social mediów potrafimy, czy mamy wręcz możliwość odzyskania go. Chcemy wiedzieć co dzieje się u naszej rodziny, korzystamy z tych rozwiązań, bo to najszybszy i najłatwiejszy sposób. Ważne jest to jakie dane umieszczamy. W jaki sposób się nimi dzielimy. A przede wszystkim kiedy się nimi dzielimy, ponieważ czas ma znaczenie, jeżeli chodzi o nasze bezpieczeństwo.

**Rafał Molenda:** Co to znaczy?

**Agnieszka Ubowska:** To informacje umieszczane na temat naszych wyjazdów. My jesteśmy za granicą i informujemy o tym cały świat, a nasz dom stoi w tym czasie przecież opuszczony. Przekazujemy różne informacje i dane w czasie rzeczywistym, a kiedy nie mamy dobrze zabezpieczonego mieszkania czy domu, to niesie ze sobą pewne ryzyko.

**Rafał Molenda:** Bardzo łatwo jest znaleźć dane, szczególnie te oficjalnie podawane. Adres domowy nie stanowi już chyba żadnej tajemnicy i bardzo łatwo go odszukać w sieci.

Przejdźmy do rzeczy. Wiemy już jakie są zagrożenia. Często zupełnie bezrefleksyjnie rozdajemy wręcz nasze dane na prawo i lewo. Ostatnio bawią mnie te oświadczenia, które można znaleźć na Facebooku, kiedy użytkownik nie wyraża zgody na wykorzystywanie jego zdjęć, z jego profilu przez samego Facebooka. Problem w tym, że niewiele osób czyta umowę podpisując ją, logując się na portalu.

**Agnieszka Ubowska:** Tak, dlatego że w wielu umowach powierzamy już swoje dane. I teraz wyrażając zgodę, czy to w sklepie, czy gdzie indziej i my wyrażamy zgodę, to zgodnie z prawem administrator danych, może z nich korzystać.

**Rafał Molenda:** I tak się dzieje. Dlatego warto czytać umowy. Przejdźmy jednak do sedna naszego spotkania. Proszę powiedzieć, jak szyfrować i jak się zabezpieczyć, żeby spać spokojnie? Zabezpieczyć swój dom, swoje mienie, swój samochód?

**Agnieszka Ubowska:** Dom jest dla nas szczególnie ważny, tym ważniejszy, że czasami zdarza się, że jesteśmy z nim związani kredytem. Dbamy o nasze mienie. Dokonujemy zabezpieczenia przez wykorzystywanie drzwi antywłamaniowych, zamków itd. Te metody mogą się nie sprawdzić. Postęp technologii rośnie, wraz, wykładniczo chyba, z postępem tych, którzy zamierzają na nasze mienie nastać. Mamy coraz lepszą świadomość, coraz lepsze narzędzia służące do tego. Sięgamy po rozwiązania coraz bardziej nowoczesne. Korzystamy z technologii, która kiedyś była dostępna jedynie dla służb czy dla wojska. Do tego typu rozwiązań zaliczymy monitoring. To monitoring, który może przybierać różne formy. Mogą to być fotopułapki, które znamy z lasów, ich celem wtedy jest wytropienie jakiejś zwierzyny. Może to być monitoring wizyjny. To mogą być też kamery umieszczone w różnych przedmiotach.

**Rafał Molenda:** Wyjaśnię tylko, że fotopułapka to kamera z czujnikiem ruchu. Aktywuje się, gdy coś w zakresie pola widzenia kamery się poruszy.

**Agnieszka Ubowska:** W zakresie bezpieczeństwa w domu, bardzo często pojawiają się kwestie monitoringu na zewnątrz. To bardzo ważny aspekt bezpieczeństwa, ale co podglądamy dzięki tym kamerom? Czy tylko zabezpieczenie naszego mienia, czy może kamera skierowana jest na okno sąsiadów. Te osoby, które poruszają się tam, mają pełne prawo do ochrony ich prywatności. W związku z tym, jeżeli mamy ustawione kamery na zewnątrz, to musimy podać do publicznej wiadomości, że taki obiekt jest monitorowany. Bardzo ważne jest to, żeby te osoby miały tego świadomość. Oczywiście najlepiej jest ustawić kamery tak, by swym zasięgiem obejmowały jedynie naszą posesję. Jeżeli mamy monitoring, to pamiętajmy, że zapisy z takiego monitoringu musimy usuwać po trzech miesiącach, chyba że prowadzone jest postępowanie dochodzeniowe. Pamiętajmy, że jeżeli nasza kamera skierowana jest na chodnik, to my zarządzamy danymi osobowymi. Nagrania takie, muszą być w odpowiedni sposób zabezpieczone.  Nikt nie może mieć do nich dostępu. Nie możemy ich w dowolny sposób też przetwarzać. Jeżeli sąsiadka przewróci się na chodniki, a nasza kamera ten fakt zarejestruje, to nie możemy wrzucić tego na You Tube. Wtedy sąsiadka będzie miała podstawy do tego, żeby nas oskarżyć.

**Rafał Molenda:** Załóżmy, że mamy już monitoring, jesteśmy zabezpieczeni, wiemy, co dzieje się za dnia i w nocy w naszym domu i przed nim i to wówczas, gdy nas nie ma. Ale mamy też mnóstwo sprzętu elektronicznego. On wymaga od nas byśmy się zalogowali, byśmy przekazali swoje dane. Jak należy się zachować i czego unikać, by nie podawać na tacy wszystkiego, takich informacji, które mogą doprowadzić do wyłudzenia pieniędzy z naszego konta?

**Agnieszka Ubowska:** Zacznę od najprostszego rozwiązania, to stosowanie oprogramowania antywirusowego. Tutaj pojawia się pewien paradoks. O ile chętnie ubezpieczamy nasze mienie w postaci samochodu czy mieszkania, o tyle rzadko mamy ochotę wysupłać niewielką sumę na zakup oprogramowania. Zdarza się tak, że na naszych komputerach znajduje się takie oprogramowanie  dzięki naszemu pracodawcy. To on zabezpiecza te dane po to, by nikt ich nie mógł wykorzystać.

**Rafał Molenda:** Często jest też tak, że jeżeli kupujemy jakiś sprzęt to on ma już zainstalowaną aplikację antywirusową. To zwykle podstawowe zabezpieczenie.

**Agnieszka Ubowska:** Musimy też pamiętać, że to podstawowe zabezpieczenie, które wgrane jest do nowego sprzętu, z reguły taki program aktywny  jest przez rok. Należy po nie sięgnąć po upływie tego czasu samemu. Jeżeli chodzi o inne zastosowania, to mamy różnego rodzaju oprogramowania  i rozwiązania techniczne. Mam tu na myśli czytniki linii papilarnych, które zabezpieczają przed korzystaniem ze sprzętu przez osoby do tego niepowołane. Takie rozwiązanie możemy znaleźć w naszych telefonach komórkowych. Stosujemy zabezpieczenia w postaci rozpoznawania właśnie linii papilarnych, twarzy, siatkówki oka. W takie rozwiązania możemy uzbroić nawet starsze urządzenia, jeżeli nie mają wbudowanych tego typu czytników.

Jeżeli chodzi o inne rozwiązania to mam na myśli takie, które monitorują to co dzieje się na komputerze. Często je stosujemy, gdy z komputera korzystają dzieci. Możemy monitorować na jakie strony wchodzą na jakie strony się logują i jakie treści zamieszczają. Wiemy, że to jest bardzo ważne. Te treści mogą bowiem lądować w różnych miejscach, a o konsekwencjach ich wykorzystywania chyba nie muszę szczególnie wspominać, znamy pewnie zjawisko memów i ich szerokiego oddźwięku. Wiemy też, że to co jest w Internecie nie ginie.

**Rafał Molenda:** To są aplikacje ogólnie dostępne.

**Agnieszka Ubowska:** Tak one są powszechne. Nie będę też wskazywać konkretnych.  Nie trzeba przy tym szpiegować wszystkiego i każdego działania. Należy to robić dla bezpieczeństwa a nie po to by szpiegować nasze dzieci i sprawdzać co one tam robią. Są systemy, które pozwalają potem znaleźć ten sprzęt. Wyposażenie sprzętu w nadajnik GPS pozwala na śledzenie i kontrolowanie, możemy w razie kradzieży namierzyć ów sprzęt. Każdy niemal współczesny zegarek elektroniczny ma lokalizator, z którego możemy z łatwością skorzystać.

**Rafał Molenda:** Czyli program antywirusowy zaktualizowany, dostosowany do naszych potrzeb. Do tego aplikacja, która kontroluje to, co dzieje się w naszym urządzeniu. Różnorodne hasła, często zmieniane.

Dom zabezpieczyliśmy, komputer również. W garażu jeszcze stoi samochód.

**Agnieszka Ubowska:** Garaż sam jest zabezpieczony, jest monitoring, drzwi antywłamaniowe, wykupiliśmy AC. A sam samochód, no to standardowe zabezpieczenia kierownicy, alarm samochodowy, nowoczesne zabezpieczenia cyfrowe, które wykorzystywane są przede wszystkim w droższych samochodach. Nadajniki GPS, dotychczas zabezpieczano w ten sposób całe samochodowe floty, szczególnie w firmach transportowych, które przewożą cenne ładunki. Obecnie po tego typu rozwiązania sięgają coraz częściej użytkownicy prywatni. W tym przypadku mamy do czynienia z różnego rodzaju kamerami umieszczonymi w samochodach, które pozwalają nagrać to, co się dzieje w tym pojeździe. I kiedy samochód ginie, możemy go namierzyć lub podsłuchać to, co ewentualnie się w jego wnętrzu dzieje. Takie urządzenia mogą działać nawet około miesiąca. To oczywiście dzięki wydajnym źródłom zasilania tych urządzeń, co pozwala im na długoterminowe działanie. Dzięki temu czasami udaje się odzyskać skradziony pojazd. Są też urządzenia, które może w Polsce nie są na tyle popularne, one pozwalają na identyfikację użytkownika. Mam na myśli czytniki linii papilarnych umożliwiających uruchomienie samochodu, lub po prostu wejście do niego.

**Rafał Molenda:** Potrafimy zabezpieczyć sprzęt, dom, samochód, co jeszcze?

**Agnieszka Ubowska:** Nasze informacje. Informacje, które przekazujemy innym.

**Rafał Molenda:** To bardzo ważne, coraz więcej jest takich stron w Internecie. Logujemy się na nie poprzez Facebooka.

**Agnieszka Ubowska:** Korzystamy przy tym z sieci publicznej.

**Rafał Molenda:** To służy temu, żeby nam, użytkownikom, było łatwiej skorzystać z jakiejś usługi w Internecie. Ale czy z każdym takim logowaniem jesteśmy bezpieczni?

**Agnieszka Ubowska:** W takich wypadkach bardzo pokutuje nasza czujność. Czasami pokazują nam się linki do stron, które otwieramy zupełnie frywolnie. Zdarza się bardzo często, że te linki są trochę kalekie, są przetłumaczone z języka angielskiego, a czasami maile, które już w swej nazwie wydają nam się podejrzane.

**Rafał Molenda:** Na co powinniśmy być wyczulenie i na co zwrócić uwagę? Jak taki podejrzany link może wyglądać a jak nie powinien wyglądać?

**Agnieszka Ubowska:** Często pojawia się bardzo wiele takich wiadomości, które w nagłówku zawierają ofertę jakiegoś zysku. Wszelkie zwroty typu: czekają na Ciebie wielkie pieniądze, otwórz, odeślij itd. Unikajmy tego typu czy to zwrotów, czy apeli, musimy być w takich wypadkach bardzo wyczuleni. To mogą być formy wyłudzeń pieniędzy, danych itd. Niestety bardzo chętnie tego typu komunikaty klikamy nawet się przy tym nie zastanawiając.

**Rafał Molenda:** I często trafiamy do osoby, która tylko na to czeka. I przejmuje taka osoba w tym momencie kontrolę nad naszym sprzętem, czy danymi wrażliwymi , czy tak?

**Agnieszka Ubowska:** Tak, przechwytywanie odbywa się właśnie w ten sposób. Przechwytywane są nasze hasła, loginy, a potem wykorzystywane.

**Rafał Molenda:** Czyli tak: zmieniliśmy hasła, nie wchodzimy na podejrzane strony, nie odpowiadamy na podejrzane wiadomości. A co z kamerami, które zamontowane są chyba w każdym urządzeniu? Czy zaklejamy te obiektywy, żeby nas ktoś nie mógł podejrzeć? Wiem, że wiele osób stosuje takie rozwiązanie. Czy też nie należy się tym przejmować, jeżeli mamy oprogramowanie antywirusowe?

**Agnieszka Ubowska:** Jeżeli jesteśmy zabezpieczeni w odpowiedni sposób, nie należy się tym przejmować. W tym przypadku zdania są oczywiście podzielone. To podobnie jak umieszczanie zdjęć w takim stroju, powiedzmy bardziej swobodnym. Wszystko jest kwestią tego na kogo trafimy po drugiej stronie i czy będzie chciał to przeciw nam to wykorzystać. W takich przypadkach powinniśmy być ostrożni, ale wszystko w ramach rozsądku.

**Rafał Molenda:** Czy coś jeszcze? Czy jesteśmy już dostatecznie dobrze zabezpieczeni, czy może coś jeszcze Pani może doradzić?

**Agnieszka Ubowska:** Załóżmy, że jesteśmy właścicielami bardzo dobrze prosperującej firmy. Nasza firma zajmuje się specjalistycznymi technologiami. Prowadzimy rozmowy na szczeblu krajowym i zagranicznym. Oczywiście zależy nam na tym, żeby nikt niepowołany nie miał dostępu do tych informacji i technologii. To są często lata naszej pracy, lata poświęceń, nakładów finansowych. Na ochronie tych danych, naszego przedsiębiorstwa bardzo nam zależy. W takiej sytuacji musimy myśleć o sprzęcie, który mamy. Należy wyposażyć komputery w dodatkowe przystawki szyfrujące, podobnie korzystajmy z szyfrujących telefonów. Oprócz tego ważne są miejsca spotkań np. z kontrahentami, zabezpieczamy takie miejsca. Czasami w pracy zdarza się, że rozmawiamy trochę zbyt głośno. Możemy być podsłuchiwani. Zabezpieczymy się przed taką ewentualnością, wyposażając się w urządzenia, które   służą do tego, żeby zakłócić fale radiowe. To generatory szumu, powodujące blokadę przesyłu sygnału. To jedno z najprostszych rozwiązań. W Szczecinie jest sklep oferujący tego typu urządzenia. To kosztuje już kilkaset złotych, zależy od czułości tego urządzenia od jego zasięgu i od sprawności. W ogóle jest cała masa urządzeń i gadżetów które możemy mieć, przypomina to trochę wyposażenie Jamesa Bonda, ale nie dajmy się zwariować, nie ze wszystkich tego typu urządzeń radzę korzystać. Należy przede wszystkim przestrzegać prawa. Są np. zestawy egzaminacyjne dla studentów, wyposażone w słuchawkę i mikrofon, urządzenia bardzo dyskretne, pozwalające przygotować się choćby do zaliczenia.

Ponadto pilnujmy swojego portfela, w którym mamy między innymi nasze dane osobowe zapisane przecież w dowodzie osobistym. W portfelu mamy też karty bankomatowe. Co roku policja odnotowuje zaginięcie tysiąca kart płatniczych, dowodów osobistych, legitymacji itd. A zgubione czy skradzione dokumenty tego typu, mogą być wykorzystywane w sposób do tego nieuprawniony.

**Rafał Molenda:** Czuję się teraz bardzo bezpieczny, będę mógł spokojnie spać, a to dzięki  Agnieszce Łubowskiej z Katedry Inżynierii Bezpieczeństwa i Energetyki Wydziału Techniki Morskiej i Transportu Zachodniopomorskiego Uniwersytetu Technologicznego.

**Agnieszka Ubowska:** Ten temat jest poruszany w ramach wykładu Uniwersytetu Trzeciego Wieku.  Z uwagi na osoby biorące udział w spotkaniach, osoby już  w wieku podeszłym, które są bardziej narażone na tego typu niebezpieczeństwa.

**Rafał Molenda:** Zapraszamy serdecznie.

**Agnieszka Ubowska:** Zapraszam na wydział.

**Rafał Molenda:** Dziękujemy za spotkanie. Pamiętajmy o tym żeby się wylogować.

**Agnieszka Ubowska:** Dziękuję.