O szczepieniach na

CYBERPRZESTĘPCZOŚĆ

i nie tylko

z nadkom. w st. spocz. Michałem Podbielskim
rozmawia podkom. Urszula Wróblewska, Zakład Kryminalny CSP

Dyrektor Biura Cyberbezpieczeństwa w Polskim Towarzystwie Ekspertów i Biegłych Sądowych. Wieloletni instruktor Akademii Policji w Szczytnie z zakresu informatyki, informatyki śledczej, cyberprzestępczości oraz cyberbezpieczeństwa. Wykładowca akademicki w Akademii Nauk Stosowanych WSGE im. A. De Gasperi w Józefowie. Twórca autorskich szkoleń z zakresu cyberprzestępczości, cyberbezpieczeństwa, informatyki śledczej oraz cyberbezpieczeństwa osobistego. Od 12 lat biegły sądowy z zakresu informatyki o specjalizacji „Telefonia komórkowa i urządzenia mobilne". Ekspert w zakresie nadzoru oraz wdrażania procedur, polityk bezpieczeństwa, analizy ryzyka, bezpieczeństwa systemów informatycznych. Odznaczony przez Prezydenta Rzeczypospolitej Polskiej „Krzyżem Zasługi za Dzielność" za uratowanie życia przy narażeniu własnego.

Droga służbowa:
2009 – wstąpienie do Policji – Wydział Patrolowy Komendy Miejskiej Policji w Ostrołęce,
2010 – Wydział Patrolowy. Ogniwo Wywiadowcze KMP w Ostrołęce,
2012 – Zespół do Walki z Korupcją, Wydział dw. z Przestępczością Gospodarczą i Korupcją KMP w Ostrołęce,
2015 – Zarząd w Radomiu Wydział w Ostrołęce Centralnego Biura Śledczego Policji,
2020–2026 – Akademia Policji w Szczytnie.

PTEiBS
POLSKIE TOWARZYSTWO EKSPERTÓW I BIEGŁYCH SĄDOWYCH

W dobie cyfrowej transformacji niemal każdy aspekt naszego życia pozostawia ślad w cyberprzestrzeni. Wraz z rozwojem nowych technologii rośnie jednak także skala zagrożeń – od oszustw internetowych i kradzieży danych po zaawansowane ataki wymierzone w instytucje publiczne oraz przedsiębiorstwa. W takich realiach szczególnego znaczenia nabierają eksperci, którzy potrafią nie tylko analizować cyfrowe ślady przestępstw, ale również skutecznie przeciwdziałać zagrożeniom. Biegli sądowi – bohaterowie drugiego planu. Ich praca wymaga nie tylko specjalistycznej wiedzy technicznej, ale również umiejętności analitycznego myślenia, dociekliwości i odpowiedzialności.

Wprowadzenie

Naszym gościem jest biegły sądowy z zakresu informatyki, ekspert z dziedziny cyberprzestępczości, cyberbezpieczeństwa oraz informatyki śledczej, Dyrektor Biura Cyberbezpieczeństwa w Polskim Towarzystwie Ekspertów i Biegłych Sądowych, były funkcjonariusz i instruktor Akademii Policji w Szczytnie, który przez lata łączył praktykę śledczą z działalnością dydaktyczną. Dzięki doświadczeniu zdobytemu zarówno w trakcie służby, jak i w związku z pełnieniem funkcji biegłego sądowego oraz w pracy na sali wykładowej, ma unikalną wiedzę na temat współczesnych wyzwań związanych z cyberprzestępczością, bezpieczeństwem informacji oraz edukacją przyszłych specjalistów. W swojej karierze zajmował się analizą cyberprzestępstw, zabezpieczaniem dowodów cyfrowych oraz wspieraniem organów ścigania i wymiaru sprawiedliwości w wyjaśnianiu skomplikowanych spraw. Dziś dzieli się swoją wiedzą z przyszłymi funkcjonariuszami i specjalistami, pokazując, że bezpieczeństwo w cyberprzestrzeni zaczyna się od świadomości, edukacji i profesjonalizmu.
Zapraszam do rozmowy o zagrożeniach cyfrowego świata, metodach działania cyberprzestępców, roli organów ścigania oraz znaczeniu świadomości społecznej w budowaniu bezpieczeństwa w sieci.

Jest Pan biegłym od przeszło 11 lat, jak wyglądała Pana droga zawodowa od służby w formacjach mundurowych do pracy biegłego sądowego?

Na wstępie chciałbym bardzo serdecznie podziękować za zaproszenie do wywiadu w Państwa kwartalniku. Niejednokrotnie czytałem Państwa czasopismo i nigdy nie przypuszczałem, że będę miał możliwość zagościć na jego stronach.
Odpowiedź na pytanie nie jest całkiem oczywista. Musimy cofnąć się o ponad 20 lat. Wówczas, jako młody człowiek, zacząłem serwisować pierwsze telefony komórkowe. Wielu czytelników zapewne już nie pamięta czasów, kiedy telefony komórkowe służyły do dzwonienia i pisania SMS oraz posiadały blokady nie tylko urządzeń, ale również blokady sieciowe, tzw. simlock. Zajmowałem się usuwaniem blokad oraz naprawą telefonów. Policja, jak i inne służby w tamtym czasie, nie miała zbyt wielu rozwiązań, a tym bardziej specjalistów w zakresie telefonów, którzy mieliby jakąkolwiek wiedzę dotyczącą obejścia zabezpieczeń czy odczytu danych z urządzeń. Najciekawsze jest to, iż do dnia dzisiejszego najwięcej problemów przysparzają właśnie te starsze telefony. Gdy prowadziłem serwis, zwracało się do mnie wiele służb, w tym Policja, o udzielenie pomocy i podzielenie się wiedzą w tym zakresie. Niejednokrotnie dokonywałem odczytu danych czy naprawy uszkodzonych telefonów przy asyście policjantów, umożliwiając dostęp do źródła dowodowego w prowadzonych sprawach. Współpraca trwała kilka lat, pomyślałem: „Dlaczego miałbym nie spróbować pracy w Policji, żeby wspierać ją od środka?”. I tak zaczęła się moja służba w szeregach Policji. Po kilku latach pracy w Wydziale Patrolowym Komendy Miejskiej Policji w Ostrołęce podjąłem decyzję o podzieleniu się moją wiedzą i doświadczeniem z innymi instytucjami, takimi jak sądy i prokuratury. Zwróciłem się do Prezesa Sądu Okręgowego w Ostrołęce z wnioskiem o ustanowienie mnie biegłym sądowym z zakresu informatyki i tak dzielę się swoją wiedzą do dnia dzisiejszego. Początkowo współpraca obejmowała rejon Sądu Okręgowego w Ostrołęce, a z czasem podjąłem współpracę na terenie całego kraju.

Każdego dnia słyszymy w przekazach medialnych o różnego rodzaju przestępstwach internetowych, w których niekiedy ofiary tracą dorobek życia. Jakie rodzaje cyberprzestępstw spotyka Pan najczęściej w swojej pracy?

Rozpoczynając swoją drogę jako biegły sądowy, myślałem, że większość spraw będzie dotyczyć przestępstw narkotykowych i związanej z tym korespondencji dotyczącej handlu, zakupu, produkcji. Na przestrzeni lat wraz z rozwojem sieci Internet zmieniała się charakterystyka przestępstw oraz danych, jakie można było uzyskać z urządzeń – i mówię tu już nie tylko o telefonach komórkowych, lecz także o komputerach, tabletach, nawigacjach czy pojazdach. Rozwój Internetu pozwolił przestępcom zmienić metody działania i przejść w świat wirtualny, by mogli popełniać przestępstwa anonimowo i bez większych obaw o ujawnienie sprawcy. Tak właśnie narodziła się cyberprzestępczość. To, co kiedyś wiązało się z bezpośrednim kontaktem przestępcy z ofiarą, teraz posiada kurtynę w postaci komputera. Jakie rodzaje cyberprzestępstw najczęściej spotykam? Niezmiennie prym wiodą oszustwa internetowe i to pod każdą możliwą postacią. Obecnie wróciła metoda oszustwa na zaliczkę lub przedpłatę. Na jednym ze znanych portali ogłoszeniowych zostają wystawiane do sprzedaży przedmioty w atrakcyjnej, ale nie przesadnie, cenie. Dochodzi do kontaktu – w tym również telefonicznego – kupującego ze sprzedającym. Kontakt telefoniczny ma utwierdzić przyszłą ofiarę o wiarygodności oferty. Sprzedający w związku z nieufnością do kupującego prosi o pełną wpłatę za przedmiot – a w razie nieufności ze strony kupującego – prosi o wpłatę zaliczki. Po wpłacie kontakt sprzedającego z kupującym zostaje utrzymany, żeby ogłoszenie jak najdłużej było aktywne i aby sprawca mógł oszukać jak najwięcej osób. Sprzedający często zmienia termin wysyłki, wskazując przeróżne problemy z tym związane. Na koniec twierdzi, że to on został oszukany i ktoś przejął jego konto bankowe, kradnąc pieniądze wpłacone za przedmiot. Oczywiście jest to totalne kłamstwo. Niekiedy kupujący odpuszczają i nie zawiadamiają Policji. Ogłoszenie zostaje zdjęte i po kilku dniach ogłoszenie powraca wystawione przez inną osobę. Należy zwrócić szczególną uwagę, że do oszustw są wykorzystywane konta istniejące kilka lat, a często również z wystawionymi innymi przedmiotami, co znacznie utrudnia weryfikację sprzedającego. Kupują na serwisach ogłoszeniowych konta z wyrobioną już historią. Zdają sobie bowiem sprawę, że są prowadzone kampanie informacyjne w mediach i Internecie ujawniające metody oszustw i pokazujące sposoby weryfikacji, dlatego też dostosowują się do tych zaleceń i instrukcji. Serwisy ogłoszeniowe

bardzo często oferują możliwość bezpiecznego kupowania z ochroną kupującego. Jeśli osoba sprzedająca nie chce się zgodzić na transakcję z ochroną, jest to pierwszy sygnał tego, że coś jest nie tak.

Biorąc pod uwagę opiniowane przez Pana sprawy – czy mógłby Pan wskazać, jakie błędy najczęściej popełniają użytkownicy Internetu, które prowadzą do utraty danych lub pieniędzy?

Niejednokrotnie w różnego rodzaju wystąpieniach ekspertów czy osób, które prowadziły profilaktykę w zakresie cyberprzestępczości słyszałem: „Nie klikaj w nieznane linki". Dziś nasze całe życie wirtualne opiera się na różnego rodzaju linkach czy kodach QR i jest ciężko nie klikać w linki. Faktycznie, wiele lat wstecz nieznane linki prowadziły do zainfekowania komputera i utraty danych czy przejęcia systemu. Obecnie cyberprzestępcy mniej korzystają z tego typu metody podpinania np. złośliwego oprogramowania pod linki, co oczywiście nie oznacza, że tego nie robią. Chodzi o pracę, jaką muszą włożyć w oszukanie ofiary i zysk, jaki osiągną. Łatwiej jest cyberprzestępcy wysłać link z fałszywą stroną, na której ofiara sama wpisze dane, które chce otrzymać przestępca, aniżeli tworzyć program, infekować komputer, obsługiwać narzędzia do odczytu i pobierania danych, co wiąże się również z łatwiejszym namierzeniem sprawcy. Cyberprzestępcy wykorzystują linki prowadzące do stworzonych przez siebie do stron internetowych, które są takie same jak oryginalne strony internetowe różnych firm (tzw. phishing) – głównie banków. Fałszywe strony są zakładane na serwerach zagranicznych, do których polskie służby mają znacznie utrudniony dostęp. Użytkownicy Internetu niestety nie sprawdzają dokładnego adresu URL strony, do której prowadzi link. Bez namysłu, bardzo często pod presją czasu, wypełniają tam żądane dane, takie jak loginy, hasła i autoryzują logowanie na aplikacjach mobilnych banków, nie odczytując informacji zawartych w tych wiadomościach. Tak więc najczęstszym błędem użytkowników Internetu jest pośpiech i brak refleksji przy wpisywaniu danych, autoryzowaniu działań wyświetlanych za pośrednictwem aplikacji na urządzeniach mobilnych, takich jak np. smartfon. Rozważmy najczęstszy scenariusz oszustwa – osoba wystawia przedmiot do sprzedaży. Ze sprzedającym kontaktuje się zainteresowany kupnem i wysyła sprzedającemu instrukcję pobrania pieniędzy poprzez logowanie się na stronie bankowości internetowej za pośrednictwem wysłanego przez niego linku. Niestety opisany przykład sprzedaży/zakupu prowadzi do utraty niejednokrotnie dużych sum pieniędzy. Oszuści przejmują władzę nad naszym kontem bankowym i dochodzi do wyprowadzenia pieniędzy z konta czy zaciągnięcia pożyczek.

Jest Pan ekspertem w dziedzinie informatyki śledczej. Jak powinien wyglądać proces zabezpieczania cyfrowych dowodów podczas postępowania przygotowawczego? Z jakimi najczęstszymi błędami można się spotkać podczas zabezpieczania dowodów?

Wydawałoby się, że proces zabezpieczania dowodów cyfrowych jest znacznie prostszy od zabezpieczania klasycznych dowodów/śladów, zważywszy na rozwój technologiczny i cyfrowy. Właśnie nie. Zabezpieczanie dowodów cyfrowych wymaga od informatyków śledczych dużej wiedzy, doświadczenia i stosowania zasad. Błędne zabezpieczenie dowodu cyfrowego może doprowadzić do modyfikacji, czyli zmiany danych, podważenia wiarygodności dowodu, a czasem nawet trwałego usunięcia danych. W swojej pracy spotkałem się z przypadkami utraty wszystkich danych przez specjalistów w dziedzinie informatyki śledczej, w tym też służb, i co gorsze – nadpisu tych danych. Dlatego podczas zabezpieczania dowodów cyfrowych każdy informatyk śledczy powinien się kierować pewnymi zasadami, które pozwolą nam na zabezpieczenie dowodu w sposób bezsporny. Zasady te obejmują: odizolowanie osób od sprzętu i uniemożliwienie jakiejkolwiek w nim ingerencji oraz zachowanie integralności danych (dowód w żaden sposób nie może ulec najmniejszej zmianie od momentu jego przejęcia), protokołowanie – informatyk śledczy powinien pamiętać o procedurze dokumentowania związanej z zatrzymaniem, dostępem, przechowywaniem, składowaniem, opakowaniem dowodu, czynności powinny zostać w pełni udokumentowane i być dostępne dla niezależnej oceny, korzystanie ze wsparcia eksperckiego w zakresie wykraczającym poza nasze umiejętności, przeszkolenie – osoba zajmująca się zabezpieczaniem dowodów cyfrowych powinna stale poszerzać swoją wiedzę, aby móc prawidłowo wykonywać czynności.
Najczęstsze błędy spotykane podczas zabezpieczania dowodów są ściśle powiązane z nieprzestrzeganiem wymienionych zasad. Jednym z takich przykładów jest podejmowanie czynności na miejscu przez funkcjonariuszy nieposiadających dostatecznej wiedzy informatycznej pozwalającej we właściwy sposób zabezpieczyć sprzęt czy dane. Prowadzi to niejednokrotnie do utraty wartości dowodowej lub co gorsze – całkowitej utraty dowodu cyfrowego. Kolejny przykład błędu popełnianego przez funkcjonariuszy to prowadzenie niepełnej dokumentacji, która nie odpowiada na kluczowe pytania: kto, kiedy i w jaki sposób posiadał dostęp do danego dowodu. Tych błędów jest znacznie więcej. Przytoczyłem te, które mają największy wpływ na wartość dowodową zabezpieczanych śladów i danych.

Współpracuje Pan z różnymi służbami. Jak wygląda współpraca biegłego sądowego z Policją, prokuraturą oraz sądem? Czy któraś z tych instytucji ma szczególne wymagania dotyczące wydawania opinii?

Cel i wymagania każdej z instytucji przy sporządzaniu opinii przez biegłego te same, czyli wydanie rzetelnej, obiektywnej i zgodnej ze stanem faktycznym ekspertyzy. Sporządzając opinię, staram się używać prostego języka,

zrozumiałego dla każdego. Należy pamiętać, że nie każdy jest specjalistą i nie musi się znać na wszystkim. Niekiedy opinia dotyczy zabezpieczenia dowodów w postaci np. zdjęć, dokumentów, plików, informacji dotyczących m.in. logowania się urządzeń czy zainstalowanych aplikacji, a czasem jest merytoryczne wypowiedzenie się w przedmiocie zagadnienia, które nie jest do końca jasne dla każdej ze stron, tak jak to jest np. w przypadku kradzieży pieniędzy z kont bankowych ofiary metodą phishingową. Wówczas należy odpowiedzieć na pytanie, czy banki dochowały wszelkich procedur bezpieczeństwa oraz na podstawie akt określić krok po kroku *modus operandi* cyberprzestępcy. Zakres spraw opiniowanych dla instytucji zlecających jest naprawdę szeroki i czasem potrafi zaskoczyć mnie samego. Współpraca z poszczególnymi instytucjami wygląda podobnie, niemniej jednak są różnice mające znaczenie z punktu widzenia biegłego. Policja w znacznej większości przesyła urządzenia wraz z pytaniami, na które biegły ma odpowiedzieć bez żadnych dodatkowych informacji. Odstępstwem od tej zasady są dwie jednostki Policji – KMP w Ostrołęce i KPP w Wałczu – z nimi współpraca jest ściślejsza, co przekłada się na wyjaśnienie wszelkich okoliczności sprawy.
Prokuratury cenią sobie bliższą współpracę. Oznacza to, że biegły jest bardziej szczegółowo wprowadzany w sprawę. Prokuratorzy bardzo często spotykają się lub dzwonią i konsultują z biegłym kwestię, jakie wartości dowodowe można wydobyć z urządzeń; a także czy istnieją inne informacje, które mogą pomóc w wyjaśnieniu sprawy lub udowodnieniu winy czy niewinności. Instytucja biegłych została stworzona właśnie w takim celu, aby przychodzili z pomocą i wspomagali instytucje swoją wiedzą i umiejętnościami.
Natomiast sąd, zwracając się z pytaniami do biegłego, udostępnia cały materiał dowodowy w postaci akt sprawy. Umożliwia to biegłemu na zebranie znacznie większej ilości informacji niezbędnych do wydania opinii i wyjaśnienie wszelkich wątpliwości.
Z doświadczenia mogę powiedzieć, że najbardziej owocna współpraca ma miejsce wówczas, gdy wprowadzimy biegłego w szczegóły sprawy. Oczywiście, czasem nie ma potrzeby większego wprowadzania biegłego w sprawę, niemniej jednak biegły, mając dostęp choćby tylko do protokołów przesłuchań, może zauważyć coś więcej niż prowadzący sprawę, w szczególności gdy biegły ma duże doświadczenie w tym zakresie.

Jakie rady może Pan przekazać osobom rozpoczynającym karierę w dziedzinie cyberbezpieczeństwa?

Bardzo często spotykam się z pytaniem: „Jesteś informatykiem i nie wiesz?". Zawsze staram się wyjaśniać, że informatyków można porównać po części do lekarzy. Na początku zdobywamy podstawową wiedzę, np. dotyczącą funkcjonowania, działania sprzętu, systemu oraz rozwiązywania podstawowych problemów, a dopiero później określamy specjalizację, jaką chcemy podążać. Informatyk będący programistą nie musi znać się na politykach bezpieczeństwa tak jak lekarz ortopeda nie musi leczyć chorób oczu. Nawet ja jako biegły czasem odmawiam wydania opinii z uwagi na brak dostatecznej wiedzy w jakiejś konkretnej specjalizacji. Nie chciałbym doprowadzić do sytuacji podważenia wydanej przeze mnie opinii.
Myślę, że najważniejsze, by osoby rozpoczynające karierę koncentrowały się właśnie nad tą konkretną specjalizacją i starały się być w niej jak najlepsze. Powinny poszerzać swoją wiedzę i umiejętności poprzez szkolenia i korzystać z wiedzy bardziej doświadczonych. Nie przejmować się porażkami i przekuwać je w sukces. Z doświadczenia wiem, że pracodawcy znacznie bardziej cenią osobę, która potrafi coś zrobić, niż taką, która zna definicje.

Czy – Pana zdaniem – przestępcy internetowi wykorzystają rozwój sztucznej inteligencji?

Od wielu lat mówiłem głośno o tym, że sztuczna inteligencja przyniesie wiele dobrego, ale również i złego. Rozwój cyberprzestępczości znacznie przyśpieszył i stanowi to ogromne wyzwanie dla służb. Dobrze, że w Polsce zostało powołane Centralne Biuro Zwalczania Cyberprzestępczości Policji, ale dziś potrzebne jest też korzystanie z wiedzy i doświadczenia praktyków policyjnych. W dobie tak bardzo rozwiniętej sztucznej inteligencji nie możemy już ufać, czy po drugiej stronie słuchawki lub monitora siedzi osoba, za którą się podaje. Oczywiście, że cyberprzestępczość korzysta z dobrodziejstwa AI. Większość poważniejszych cyberprzestępców korzysta z w pełni zautomatyzowanych funkcji sztucznej inteligencji. Przestępcy nie tworzą nowych rodzajów ataków, korzystają z tych już sprawdzonych, ale sztuczna inteligencja pomaga dziś przestępcom w automatyzacji, skalowaniu i zwiększaniu wiarygodności istniejących oszustw. Na ataki z użyciem sztucznej inteligencji narażony jest zarówno przeciętny człowiek, jak i instytucje. Możemy sobie wyobrazić sytuację, w której dzwoni do nas przełożony i prosi o wykonanie jakiejś czynności. W słuchawce oczywiście słyszymy jego głos i nie mamy żadnej wątpliwości, że po drugiej stronie jest ta właśnie osoba. Bezrefleksyjnie wykonujemy jego polecenia, co sprawia, że przestępca osiąga swój skutek. Każdy z nas widział efekty *deepfake* obrazu i głosu, pozostaje kwestią czasu, jak *deepfake'owy* głos będzie wykorzystywany masowo. Kolejnym przykładem wykorzystania sztucznej inteligencji może być przeprowadzenie oszustwa biznesowego (BEC – Business Email Compromise). Rozważmy przykład przesłania na skrzynkę służbową wiadomości email przesłanej masowo do wielu pracowników, funkcjonariuszy opatrzoną wszystkimi cechami naszego przełożonego. W wiadomości załączony został załącznik, a z treści wiadomości możemy wyczytać o przesłaniu zestawienia premii, dodatków z listą osób w celu transparentności przyznawania nagród. Takiego badania nie przeprowadziłem, ale myślę, że znaczna większość otworzyłaby załącznik, nawet z ciekawości. Wraz z otwarciem załącznika można doprowadzić do zainfekowania komputera, a to z kolei otwiera dalszą drogę cyberprzestępcy do osiągnięcia z góry założonego celu.
W praktyce człowiek pozostaje najsłabszym ogniwem, a AI sprawia, że manipulowanie ludźmi staje się tańsze, szybsze i bardziej przekonujące. Dlatego

umiejętność weryfikacji informacji i tożsamości rozmówcy jest dziś jednym z najważniejszych elementów cyberbezpieczeństwa.

Pracując na co dzień z przestępczością internetową, specjaliści napotykają wiele problemów. Które przypadki cyberprzestępczości, z jakimi miał Pan do czynienia, były najtrudniejsze?

Najtrudniejsze nie są te, które sprawiają problemy techniczne, a te, które są ciężkie moralnie, np. pedofilia. Sprawy tej kategorii przysparzają najwięcej problemów, żeby móc się od nich zdystansować. To biegły jest na tej pierwszej linii, gdzie musi przygotować materiał dowodowy dla prokuratury czy Policji. Wiąże się to niestety z wyselekcjonowaniem m.in. materiałów w postaci zdjęć czy filmów. Są oczywiście gotowe rozwiązania w postaci odpowiedniego oprogramowania, które pozwala na wyodrębnienie takiej zawartości, lecz nie są zbyt dokładne. Dlatego muszę osobiście dokonać skrupulatnej analizy danych, by odnaleźć wszystkie dowody oraz osoby pokrzywdzone. Prowadząc sprawy dotyczące pedofilii, człowiek nie zdaje sobie sprawy, jak przebiegli i bez kręgosłupa moralnego są pedofile. Podczas moich wystąpień w szkołach zawsze staram się uświadamiać dzieci, młodzież, ale również rodziców o tego typu zagrożeniach. Staram się przedstawiać sprawy, które były opiniowane – oczywiście w zakresie, w jakim je mogę przedstawić – i pokazywać, jak przestępcy sterują i manipulują dziećmi, żeby osiągnąć swój cel. Zawsze zaczyna się niewinnie: zaczepka przez komunikator internetowy, rozmowy, zrozumienie, te same zainteresowania, dostępność na każde zawołanie i próba zdystansowania dziecka od rodziców. Dlatego wprowadźmy delikatną kontrolę, co nasze dzieci piszą i z kim. Analizując sprawy, zauważyłem, że zawsze były wysyłane przez dziecko sygnały do rodziców, osób bliskich, że coś jest nie tak. Odzwierciedlenie ma to później w rozmowach bardzo często z innym dzieckiem, kolegą, koleżanką, którym to dziecko zwierza się, że nikt go nie rozumie i nie potrafił wysłuchać.

Od jakiegoś czasu można wyraźnie zauważyć, że na świecie przyśpieszył rozwój technologiczny. Parędziesiąt lat wstecz jedynym urządzeniem do korzystania z Internetu był komputer. Obecnie korzystamy ze smartfonów, tabletów i innych urządzeń pozwalających na łączenie się z siecią Internet. Jak Pan uważa, czy urządzenia mobilne są obecnie większym źródłem zagrożeń niż tradycyjne komputery? A może są inne urządzenia, które mogą przynieść równie poważne zagrożenia jak komputer czy smartfon?

Wszystko zależy od tego, co chce osiągnąć przestępca. Są pewne typy przestępstw, jak np. ransomware (blokowanie dostępu do danych komputera poprzez zaszyfrowanie), gdzie przestępca będzie miał na celu osiągnięcie jak największej korzyści finansowej – stosowane głównie na komputerach, serwerach. Urządzenie mobilne jest niezbędne przy zastosowaniu metody phishingu, gdzie ofiara klika w link przesłany przez sprawcę i zostaje przekierowana na stronę identyczną jak strona banku, z żądaniem zalogowania. W tym momencie jest niezbędny smartfon w celu uwierzytelnienia logowania się przestępcy do bankowości. Czasem pewnego typu metody stosuje się i na komputery, i na urządzenia mobilne – mówię o zdalnym pulpicie. Dochodzi do kontaktu rzekomego pracownika banku, który informuje o podejrzanych działaniach na naszym koncie bankowym, po czym proponuje zainstalowanie aplikacji umożliwiającej blokowanie tych działań. Aplikacja, którą proponuje sprawca, to nic innego jak zdalny pulpit umożliwiający mu przejęcie pełnej kontroli nad naszym urządzeniem. Analizując skuteczność cyberataków, myślę, że zwiększy się liczba zagrożeń wobec smartfonów. Niejednokrotnie uświadamiam słuchaczom, że dziś naszą tożsamością nie jest tylko imię, nazwisko, wizerunek itp. Naszą tożsamością jest również smartfon. Nasze urządzenia zawierają ogrom informacji, autoryzują transakcje czy wytyczają drogę. Kto może znać nas lepiej niż nasz smartfon. Przez niego prowadzimy rozmowę, wysyłamy wiadomości, dokonujemy płatności, a niektórzy popełniają przestępstwa. Smartfony wiedzą o nas wszystko. Ale cyberprzestępstwa można popełnić na wiele różnych sposobów i przy wykorzystaniu różnego rodzaju urządzeń, takich jak np. IoT – internet of things (z ang. internet rzeczy). Na co dzień wykorzystujemy rzeczy podłączone do Internetu, nie zastanawiając się nad odpowiednim zabezpieczeniem, więc można je łatwo wykorzystać do ataków.

Jak wygląda analiza telefonu lub komputera zabezpieczonego jako materiał dowodowy?

Przy wykonywaniu czynności najważniejsze jest odpowiednie zachowanie na miejscu oraz dokumentowanie. Na zajęciach z prowadzenia czynności na miejscu podczas zabezpieczania danych zawsze podkreślałem, iż odpowiednie dokumentowanie i wykonywanie czynności pozwoli na uniknięcie jakichkolwiek zarzutów dotyczących umyślnego popełniania błędów czy podważenia wartości dowodowych. Błędy czasem się zdarzają i jest to naturalne, ważne, by było ich jak najmniej lub w ogóle, a jeśli już są – to żeby inny specjalista lub biegły mógł je naprawić. I tu bardzo pomocna jest dokumentacja. Zapoznając się z nią, szybko można wyłapać, do jakiego błędu doszło i w jaki sposób go naprawić.
Każdorazowo przy zabezpieczaniu danych z urządzeń jest niezbędny odpowiedni sprzęt – programy informatyki śledczej, pokrowce blokujące sygnał, przewody i powerbanki, ale również śrubokręty i inne narzędzia niezbędne czasem do rozebrania urządzenia. Najważniejsze jest, by nie doszło do naruszenia integralności danych zawartych

w urządzeniach, dlatego w pierwszej kolejności tworzymy kopię binarną pamięci urządzenia, a dopiero po tej czynności możemy przejść do analizy danych zawartych w kopii. Należy pamiętać, że w idealnym świecie kopie takie powinny być trzy – jedna do prowadzenia badań, druga kopia bezpieczeństwa w razie popełnienia błędu przez badającego i trzecia do udostępniania wraz z materiałami sprawy. W każdym razie jedna z kopii powinna pozostać bez otwierania dla bezpieczeństwa danych. Mając kopię, można przejść do analizy danych. W tym miejscu ma znaczenie, jakie dane chcemy uzyskać z pamięci urządzenia. Czasem wystarczą programy do przeszukiwania pamięci, ale czasem nawet jest niezbędne postawienie kopii na nowym dysku i uruchomienie go w formie działającego systemu. Wszystko zależy od zlecenia. Najważniejsze, by odpowiednio dokumentować postęp prac.

Jest Pan autorem wielu autorskich szkoleń dla różnych grup zawodowych. Uczestniczył Pan w licznych konferencjach, debatach i spotkaniach profilaktycznych w szkołach. Jakie znaczenie ma edukacja społeczeństwa w zakresie cyberbezpieczeństwa?

Myślę, że społeczeństwo jest coraz bardziej świadome zagrożeń w sieci. Niemniej jednak uważam, że znacznie za mało jest prowadzonych kampanii informacyjnych o zagrożeniach. Przestępcy korzystają niezmiennie z tych samych metod, modyfikując i dostosowując się do tego, co dzieje się na świecie, w państwie, w mieście. Opinia publiczna powinna być częściej informowana o aktualnych trendach cyberprzestępstw, które należy przekazywać w sposób zrozumiały dla przeciętnej osoby. Trzeba pamiętać, że większość skutecznych cyberataków wykorzystuje błędy ludzkie, a nie luki techniczne. Prowadzenie edukacji na szerszą skalę w znacznym stopniu ogranicza skuteczność oszustw, chroni gospodarkę i instytucje, zwiększa bezpieczeństwo dzieci i młodzieży. Jak można zauważyć, edukacja w tym zakresie przynosi same korzyści. Technologia rozwija się szybciej niż świadomość społeczna. Narzędzia oparte na AI, deepfake i coraz bardziej przekonujące oszustwa internetowe sprawiają, że edukacja nie może być jednorazowym zastrzykiem wiedzy. Powinna być procesem ciągłym, obejmującym dzieci, dorosłych i seniorów. Można powiedzieć, że w cyberbezpieczeństwie edukacja pełni podobną rolę jak szczepienia w zdrowiu publicznym: nie eliminuje wszystkich zagrożeń, ale znacząco zmniejsza ich skalę i skutki.

Czy według Pana dzieci i młodzież są dziś bardziej narażone na cyberprzestępczość niż dorośli?

Niezależnie od tego, czy są to dzieci, młodzież czy dorośli każdy z nas jest w takim samym stopniu narażony na cyberprzestępczość. Różnica dotyczy tylko rodzaju przestępstwa.

Najmłodsi w społeczeństwie najbardziej są narażeni na *grooming* – próba nawiązania przez dorosłego więzi z dzieckiem w celu wykorzystania seksualnego oraz *troll parenting* – zachowanie rodziców polegające na dzieleniu się w internecie materiałami ośmieszającymi ich dzieci lub ukazującymi je w sytuacjach trudnych, wstydliwych, a nawet upokarzających. Rodzice często nie zdają sobie sprawy, że mogą w ten sposób wyrządzić dziecku krzywdę.

Młodzież narażona jest najbardziej na cyberprzemoc ze strony rówieśników. Niezmiennie co jakiś czas słyszymy o znęcaniu się psychicznym nad rówieśnikami – o szkalowaniu, wyśmiewaniu i wykluczaniu kogoś z życia społecznego. Takie zachowanie ze strony rówieśników kończy się tragedią. Tragedią dla nastolatka, ale również rodziców, bliskich. Powinniśmy nieustannie o tym przypominać i uświadamiać.

Dorośli narażeni są na oszustwa internetowe, ale nie tylko. Bardzo niebezpiecznym zjawiskiem jest *sextortion* – szantaż seksualny poprzez wykorzystanie niefizycznej formy przymusu w celu wymuszenia przysług seksualnych lub pieniędzy od ofiary. Tego typu cyberprzestępstwo może dotknąć zarówno dorosłych, młodzież, ale również dzieci. Niejednokrotnie dzielimy się zdjęciami z osobami, które „znamy" tylko przez Internet, co może prowadzić do wykorzystania tych materiałów przeciwko nam. Zaczyna się od jednego zdjęcia, następnie przestępca szantażuje ofiarę i wymusza kolejne zdjęcia, kończąc na żądaniach pieniędzy.

Nie zapomnijmy o naszych seniorach, którzy są niejednokrotnie bardziej narażeni niż dzieci, młodzież czy dorośli. Grupa ta jest najchętniej atakowana z uwagi na niedostateczną wiedzę i skłonność do obdarowywania innych dużym zaufaniem.

W świecie, w którym coraz większa część naszego życia przenosi się do Internetu, bezpieczeństwo cyfrowe staje się równie ważne jak bezpieczeństwo w świecie rzeczywistym.

Obecnie Polska jest bardziej narażona na cyberataki. Każdego dnia dochodzi do kilkudziesięciu tysięcy, a nawet kilku milionów prób ataków na różne instytucje. Jakie są najczęstsze metody działania cyberprzestępców wobec instytucji publicznych?

W większości przypadków atak na instytucje publiczne jest ukierunkowany na dwa cele: pozyskanie danych i zysk finansowy. Ostatnio można również spotkać się ze szpiegostwem obcych krajów. Żeby atak był skuteczny i osiągnął zamierzony cel, sprawcy wykorzystują różne metody, a czasem łączą kilka z nich.

Jedną z nadal najskuteczniejszych metod jest *phishing* i *spear phishing* (spersonalizowany, dokładnie zaplanowany socjotechniczny atak). *Spear phishing* jest szczególnie niebezpieczny, ponieważ wiadomości są przygotowywane pod konkretną osobę lub urząd.

Kolejną z metod wykorzystywanych przez przestępców jest *ransomware* (złośliwe oprogramowanie szyfrujące dane), niejednokrotnie infekowany poprzez użycie metody *spear phisingu*.
Jedną z najwcześniej aktywnie wykorzystywanych metod przez przestępców na szerszą skalę były ataki DDoS – *Distributed Denial of Service* (z ang. rozproszona odmowa usługi). Polega na zalaniu atakowanego systemu bardzo dużą liczbą zapytań z wielu różnych źródeł. Celem jest przeciążenie systemu.
Instytucje planujące wdrożenie polityki bezpieczeństwa powinny mieć na względzie, że wiele poważnych incydentów zaczyna się od pozornie prostego błędu człowieka – kliknięcia w fałszywy link lub użycia słabego hasła. Dlatego obok technologii kluczową rolę odgrywają procedury i świadomość użytkowników.

Skoro rozmawiamy o atakach na instytucję, proszę wskazać, jakie błędy organizacyjne najczęściej występują w administracji publicznej, jeśli chodzi o bezpieczeństwo IT?

Znaczna większość instytucji jest dobrze zabezpieczona pod względem technologicznym. Posiada sprzęt oraz oprogramowanie czuwające nad bezpieczeństwem. Najczęściej występują błędy organizacyjne. Problemem jest podejście pracowników. Traktują cyberbezpieczeństwo wyłącznie jako problem działu IT, a bezpieczeństwo powinno być odpowiedzialnością całej instytucji. W momencie gdy kierownictwo nie angażuje się w zarządzanie ryzykiem, procedury bezpieczeństwa często pozostają tylko formalnością. Słabym punktem instytucji jest brak ciągłości i powtarzalności szkoleń. Ciągłe uświadamianie pracowników oraz wskazywanie najnowszych trendów cyberprzestępców może pomóc rozpoznać ataki. Instytucje zapominają również o aktualizacji procedur i polityk bezpieczeństwa. Widziałem polityki bezpieczeństwa przestarzałe i nieaktualizowane od wielu lat. Kolejnym błędem jest nadawanie nadmiernych uprawnień użytkownikom. Posiadają oni często dostęp do znacznie większej liczby systemów oraz danych, niż potrzebują do wykonywania swoich obowiązków. Narusza to zasadę najmniejszych uprawnień (*least privilege*). Instytucje nie testują planów reagowania na incydenty. Mają procedury reagowania, ale nigdy ich nie testują. W efekcie podczas wystąpienia rzeczywistego incydentu pojawia się chaos, opóźnienia i niejasny podział odpowiedzialności. Inny ważny błąd, jaki można zauważyć, to niedostateczne wsparcie kierownictwa. Cyberbezpieczeństwo postrzegane jest wyłącznie jako koszt i zbędny wydatek. Jest to jeden z najczęściej wskazywanych problemów przez audytorów i specjalistów ds. bezpieczeństwa.
Największe ryzyko w instytucjach czy administracji publicznej zwykle nie wynika z braku konkretnych narzędzi, lecz z połączenia trzech czynników: niewystarczającej świadomości, słabego zarządzania procesami bezpieczeństwa oraz niedostatecznego nadzoru nad ryzykiem. Dlatego skuteczne cyberbezpieczeństwo jest przede wszystkim zagadnieniem organizacyjnym i zarządczym, a dopiero w drugiej kolejności technologicznym.

Pracował Pan jako instruktor i szkoleniowiec w Akademii Policji w Szczytnie. Był Pan jedną z osób tworzących program studiów dla funkcjonariuszy CBZC. Jak wygląda proces szkolenia funkcjonariuszy w zakresie cyberbezpieczeństwa, cyberprzestępczości?

Obecnie każda z instytucji, w tym Policja, boryka się z brakiem specjalistów w zakresie cyberbezpieczeństwa i cyberprzestępczości, dlatego krok w kierunku utworzenia studiów z tego zakresu był jak najbardziej uzasadniony i oczywisty. Studia pierwszego stopnia są uzupełniane drugim stopniem, gdzie wiedza jest uszczegółowiana i uzupełniana. Treści programowe są merytoryczne, niemniej jednak wydaje się konieczne jeszcze kompleksowe rozwiązanie podpierające teorię cykliczną praktyką. Akademia Policji w Szczytnie ma możliwości do wprowadzenia stałych rozwiązań i wdrożenia szkoleń czysto praktycznych, które uświadomią funkcjonariuszom, jak działa przestępstwo z punktu widzenia sprawcy. Stworzenie odizolowanego środowiska do przeprowadzania ataków i zbierania śladów informacji jest niezbędne dla ustalenia sprawcy. Do tego potrzebni są wykładowcy posiadający wiedzę praktyczną z konkretnych specjalizacji. Przy tworzeniu praktycznego programu należałoby także korzystać ze wsparcia odpowiednich osób, mających dostateczną wiedzę i umiejętności. Niemniej jednak Akademia Policji w Szczytnie zmierza w dobrym kierunku, aczkolwiek trochę za wolno. Funkcjonariusze są głodni wiedzy i chcą tę wiedzę zdobywać i poszerzać.

Summary

Resilience to cybercrime and more... Interview with court expert in the field of computer forensics

In this interview, the Director of the Cybersecurity Office at the Polish Society of Experts and Court Experts (Polish: Polskie Towarzystwo Ekspertów i Biegłych Sądowych), a former police officer, a court expert in IT, an expert in the supervision and implementation of security procedures and policies, risk analysis and the security of IT systems, answers questions about the types of crimes he most often encounters in his work, as well as about the directions of cybercrime development. He emphasizes that the development of AI has already contributed to the automation, scaling and increasing the credibility of fraud in cyberspace. He also announces the next stages of development of AI-based crime. He points out common mistakes made by Internet users that are exploited by criminals and lead to loss of data or money.
As an expert in the field of computer forensics, he discusses the process of securing digital evidence during pre-trial proceedings, as well as the principles of securing digital evidence and the most common mistakes made by investigators in this area. He emphasizes the need to introduce into the training programs of police officers dealing with cybercrime regular, purely practical exercises conducted by lecturers with practical knowledge and skills in specific specializations.
He also explores issues related to cooperation between court experts and the Police, prosecutors, and courts. He pays special attention to the difficult issues of securing evidence and preparing expert opinions in cases involving pedophilia. He highlights the role of continuous education of the entire society regarding current threats posed by the Internet, with particular emphasis on the threats to which the youngest and seniors are exposed. Due to the rapidly growing number of cyberattacks on public administration and other institutions and companies, he calls for a responsible approach to cybersecurity by management and employees, as well as for compliance with policies and procedures in the field of the security of IT systems.

Tłumaczenie: Beata Pepłowska