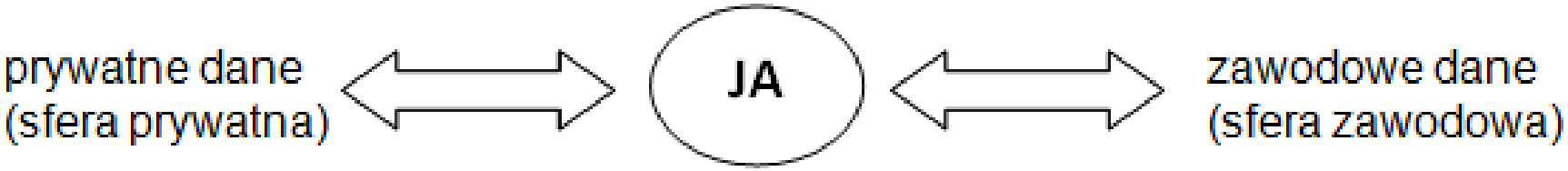
Prywatne i zawodowe materiały elektroniczne pozostające w dyspozycji służb ochrony państwa

mgr inż. Marcin Żukowski

Ekspert ds. bezpieczeństwa IT

Projekt Badawczo- Rozwojowy realizowany na rzecz bezpieczeństwa i obronności Państwa współfinansowany ze środków Narodowego Centrum Badań i Rozwoju
„MODEL REGULACJI JAWNOŚCI I JEJ OGRANICZEŃ W DEMOKRATYCZNYM PAŃSTWIE PRAWNYM”

Interakcja prywatne – zawodowe dane



„Moje dokumenty” „Moje zdjęcia” „Moje kontakty”

Wartość danych prywatnych i zawodowych

„Bardzo trudno jest zauważyć kradzież informacji (danych cyfrowych). Przy innych formach kradzieży coś fizycznie ginie. Informację można natomiast skopiować – ukraść w taki sposób, że niczego nie brakuje. Dalej ją masz, jednak nie ma ona już żadnej wartości”.

Heffernan z R.J. Heffernan Associates Inc., 2001

Wartość danych prywatnych i zawodowych

Czy moja wartość „zanika” (poczucie wartości) jeżeli wiem, że ktoś te dane ma?

Jakie to są dane, że jestem skłonny je odzyskać (choćby ich kopię)?

Dlaczego niektórym osobom nie zależy już na nich?

Projekt Badawczo- Rozwojowy realizowany na rzecz bezpieczeństwa i obronności Państwa współfinansowany ze środków Narodowego Centrum Badań i Rozwoju
„MODEL REGULACJI JAWNOŚCI I JEJ OGRANICZEŃ W DEMOKRATYCZNYM PAŃSTWIE PRAWNYM”

Elektroniczne materiały prywatne (wymiar wirtualny)

To co mnie identyfikuje (chcę być anonimowy):

• **moje dane osobowe** (w rozumieniu UoODO za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej … albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne)
• **moje dane wrażliwe** (w rozumieniu UoODO za dane osobowe wrażliwe to dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również dane o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz dane dotyczące skazań i innych orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym)
• **adres IP komputera / urządzenia**
• **prywatna poczta / konta na portalach społecznościowych czy forach**
• **używanie TORa (anonimowy komputer w sieci)**

Elektroniczne materiały prywatne (wymiar wirtualny)

To z kim się komunikuję (chcę mieć tajemnicę komunikowania się):

- **książka adresowa (kontaktowa)**
- **moja rodzina i znajomi na portalach społecznościowych**
- **historia rozmów (Facebook / chat / gadu-gadu)**
- **przynależność do kręgów / grup**
- **wpisy na portalach internetowych (wyrażanie swoich opinii)**
- **odwiedzane strony WWW**
- **frazy wyszukiwane w wyszukiwarkach internetowych**

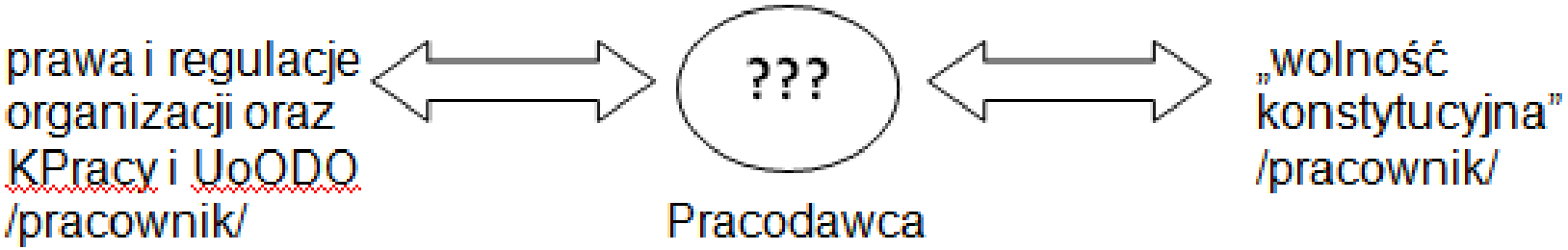
Elektroniczne materiały prywatne (wymiar wirtualny)

To co mam (nie chcę, aby ktoś wiedział o moich dokumentach):

- **zrzuty i kopie przelewów bankowych**
- **moje wpłaty i wypłaty na kontach bankowych, zeznania PIT**
- **zapisane hasła i PINy do kart bankomatowych / kredytowych**
- **wszelakie rachunki**
- **zdjęcia i filmy prywatne**
- **sprzedaż produktów na portalach aukcyjnych**
- **moje dokumenty w chmurze (np. Google Documents, Flickr)**
- **wirtualna waluta BitCoin (kryptowaluta)**
- **moja twórczość**

Elektroniczne materiały zawodowe (wymiar wirtualny)

W dobie pracy zdalnej (usługi VPN – sieć firmowa w domu / BYOD – używaj swoje prywatne urządzenie w ramach pracy zawodowej) sfera prywatna mocniej dotyka sfery zawodowej.



Elektroniczne materiały zawodowe (wymiar wirtualny)

To co mnie identyfikuje:
- kim jestem i co robię w organizacji?
- dane organizacji

To z kim się komunikuję:
- kontakty ze współpracownikami / klientami /przełożonymi / kontrahentami oraz ich preferencje (ich dane osobowe wrażliwe?)
- prywatne rozmowy z ww. osobami

To co mam w zawodowych dokumentach:
- dane klientów / kontrahentów
- finanse firmy (kondycja firmy)
- projekty / raporty / opinie
- zdjęcia ze spotkań służbowych

Tajemnica służbowa

Tajemnica służbowa – termin prawny, który w prawie polskim był zdefiniowany w ustawie z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych, a zniesiony został ustawą z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych. Oznaczał on informację niejawną niebędącą tajemnicą państwową, uzyskaną w związku z czynnościami służbowymi albo wykonywaniem prac zleconych, której nieuprawnione ujawnienie mogłoby narazić na szkodę interes państwa, interes publiczny lub prawnie chroniony interes obywateli albo jednostki organizacyjnej (art. 2 pkt 2).

Prywatne i zawodowe materiały elektroniczne - dane telekomunikacyjne

Dane bilingowe: kiedy?, z kim? (kontakty), ile czasu?, smsy, mmsy, fax

Dane użytkownika: służące identyfikacji osoby oraz adresu dostarczania rachunku

Dane lokalizacyjne, po: GPS, Wi-Fi, nadajnikach sieci komórkowej oraz sieć stacjonarna i kablowa, telefon stacjonarny

Dane identyfikujące usługę (ale też skąd była inicjacja połączenia i do którego skierowano połączenie), dostęp do Internetu, poczty, telefonii internetowej, aplikacji internetowych (np. GooglePlay), telewizji cyfrowej

Prywatne i zawodowe materiały elektroniczne - dane telekomunikacyjne

Treść zapytania: proszę o udostępnienie historii połączeń wykonanych z kart telefonicznych o numerach (xxx).

Treść zapytania: proszę o przesłanie wykazu połączeń z n/wym. numeru za maksymalny okres retencji danych: (xxx).

Treść zapytania: proszę o udostępnienie historii połączeń inicjowanych z terenu całej Polski oraz przychodzących od abonentów o numerach: (xxx).

Prywatne i zawodowe materiały elektroniczne

Elektronicznych materiałów prywatnych i zawodowych jest potencjalnie ogromna ilość, które są i **były** przetwarzane w urządzeniach elektronicznych i w elektronicznych środkach komunikacji oraz zapisywane na nośnikach danych (zewnętrznych i wewnętrznych).

Czy można powiedzieć o kradzieży wirtualnej tożsamości ?!

Informacja o wynikach kontroli NIK kpb-p/12/191 (2 czerwca 2013)

Uzyskiwanie i przetwarzanie przez Uprawnione podmioty danych z bilingów, informacji o lokalizacji oraz innych danych, o których mowa w art. 180 c i d Ustawy prawo telekomunikacyjne.

Kontrolą objęto Agencję Bezpieczeństwa Wewnętrznego, Centralne Biuro Antykorupcyjne, wybrane jednostki policji (Komendę Główną Policji, 3 Komendy Wojewódzkie), Komendę Główną Straży Granicznej, Służbę Kontrwywiadu Wojskowego, Żandarmerię Wojskową, Ministerstwo Finansów (służba celna oraz departament wywiadu skarbowego), 3 wybrane Sądy Okręgowe oraz 4 Prokuratury Okręgowe, a także Urząd Komunikacji Elektronicznej.

Informacja o wynikach kontroli NIK kpb-p/12/191 (2 czerwca 2013)

Lp.	Jednostka	Podstawa prawna	Cel sięgania po dane	Typy przestępstw (ograniczenia)
1.	Agencja Bezpieczeństwa Wewnętrznego	art. 28 ustawy o ABW	realizacja wszelkich zadań ustawowych[27]	godzące w bezpieczeństwo wewnętrzne państwa oraz jego porządek konstytucyjny[28]
2.	Centralne Biuro Antykorupcyjne	art. 18 ustawy o CBA	realizacja wszelkich zadań ustawowych[29]	korupcyjne, przeciwko instytucjom państwowym i samorządowym, godzące w interesy ekonomiczne państwa
3.	Policja	art. 20c ustawy o Policji	zapobieganie i wykrywanie przestępstw	wszystkie przestępstwa

Informacja o wynikach kontroli NIK kpb-p/12/191 (2 czerwca 2013)

Lp.	Jednostka	Podstawa prawna	Cel sięgania po dane	Typy przestępstw (ograniczenia)
4.	Służba Kontrwywiadu Wojskowego	art. 32 ustawy o SKW i SWW	realizacja wszelkich zadań ustawowych[30]	przestępstwa popełniane przez żołnierzy pełniących czynną służbę wojskową
5.	Straż Graniczna	art. 10b ustawy o SG	zapobieganie i wykrywanie przestępstw	wszystkie przestępstwa, których zwalczanie pozostaje we właściwości SG[31]
6.	Żandarmeria Wojskowa	art. 30 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych	zapobieganie i wykrywanie przestępstw	wszystkie przestępstwa popełnione przez żołnierzy, pracowników cywilnych wojska (w określonych przypadkach), osoby przebywające na terenach wojskowych[32]

Informacja o wynikach kontroli NIK kpb-p/12/191 (2 czerwca 2013)

Dane liczbowe dotyczące zakresu i ilości zapytań złożonych przez ABW w okresie od 1 stycznia 2011 r. do 30 czerwca 2012 r. przedstawiały się następująco:

Rok	Ilość zapytań dotyczących:				Zapytania ogólne	RAZEM
	lokalizacji	wykazu połączeń	ustaleń końcowych użytkowników	ustaleń nr. użytkowanych przez osobę		
1.	2.	3.	4.	5.	6.	7.
2011	7.000	65.000	30.681	20.319	3.250	126.250
2012 (do 30 IV)	3.684	25.302	14.972	8.039	1.429	53.426

CBA Rok	Zapytania o				Razem
	wykazy połączeń	dane abonenta	dane lokalizacyjne	pozostałe sprawdzenia (w tym IP, IMSI)	
1.	2.	3.	4.	6.	7.
2011	6 133	62 054	2 028	553	70 808
01.01. – 30.06.2012	2 981	68 343	751	423	72 498

Informacja o wynikach kontroli NIK kpb-p/12/191 (2 czerwca 2013)

Dane liczbowe dotyczące zakresu i liczby zapytań złożonych przez Policję w 2011 r. przedstawiały się następująco[44]:

Rok	Zapytania o:					Razem
	wykazy połączeń	dane abonenta	dane lokalizacyjne	użytkowników zakończenia sieci (abonent IP)	inne (biling z BTS itp.)	
1.	2.	3.	4.	5.	6.	7.
2011	632 606	610 156	102 067	59 902	43 880	1 448 611

Procentowe zestawienie liczby zapytań telekomunikacyjnych KGP odpowiednio w 2011 r. i w I półroczu 2012 r. przedstawia się następująco:

Rodzaj zapytania	2011 r.	2012 r. (I-IV)
lokalizacja telefonów komórkowych	2,3%	4,2%
wykaz połączeń (bilingi, IMEI, MSISDN itp.)	28,1%	35,9%
abonenci (MSISDN, IMEI, SIM, IMSI, REGON, NIP, PESEL, Adres)	68,8%	57,4%
inne (biling z BTS itp.)	0,8%	2,5%
użytkownik zakończenia sieci (abonent IP)	0,4%	0,2%

Informacja o wynikach kontroli NIK kpb-p/12/191 (2 czerwca 2013)

Na podstawie przedłożonych przez Komendanta Głównego Straży Granicznej zestawień zrealizowanych przez Straż Graniczną zapytań o dane telekomunikacyjne stwierdzono, że okresie od 1 stycznia 2011 r. do 30 czerwca 2012 r., upoważnieni funkcjonariusze Straży Granicznej występowali na podstawie art. 10b ustawy o Straży Granicznej do przedsiębiorców telekomunikacyjnych 521 903 razy, w tym Komenda Główna 8 707. Struktura skierowanych zapytań przedstawia się następująco:

Rok	Zapytania o:				Razem
	wykazy połączeń	dane abonenta	dane lokalizacyjne	Inne	
1.	2.	3.	4.	5.	7.
Od 01.01.2011 r. do 30.06.2012 r.	220 694	228 654	60 315	12 240	521 903

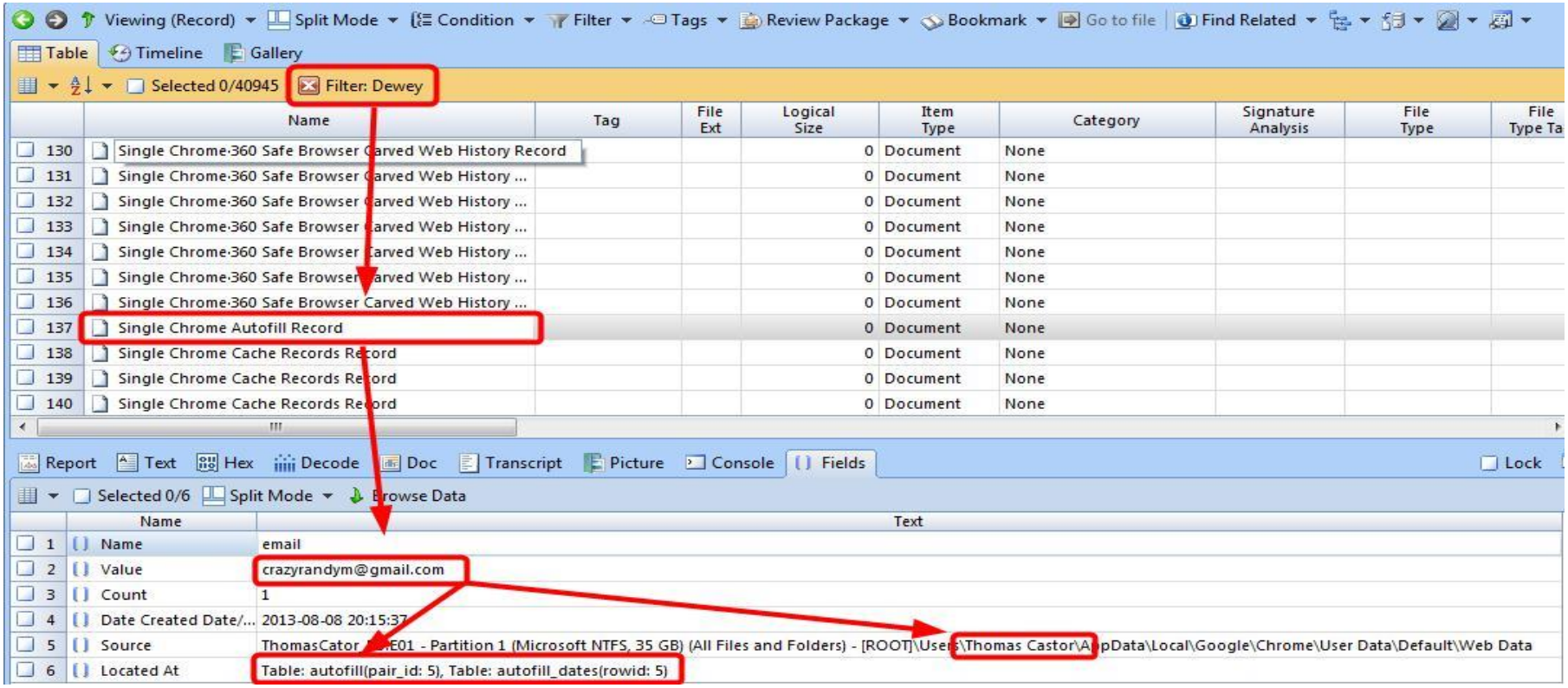
Przykład programu Encase (informatyka śledcza)

Cyt. za firmą Mediarecovery:

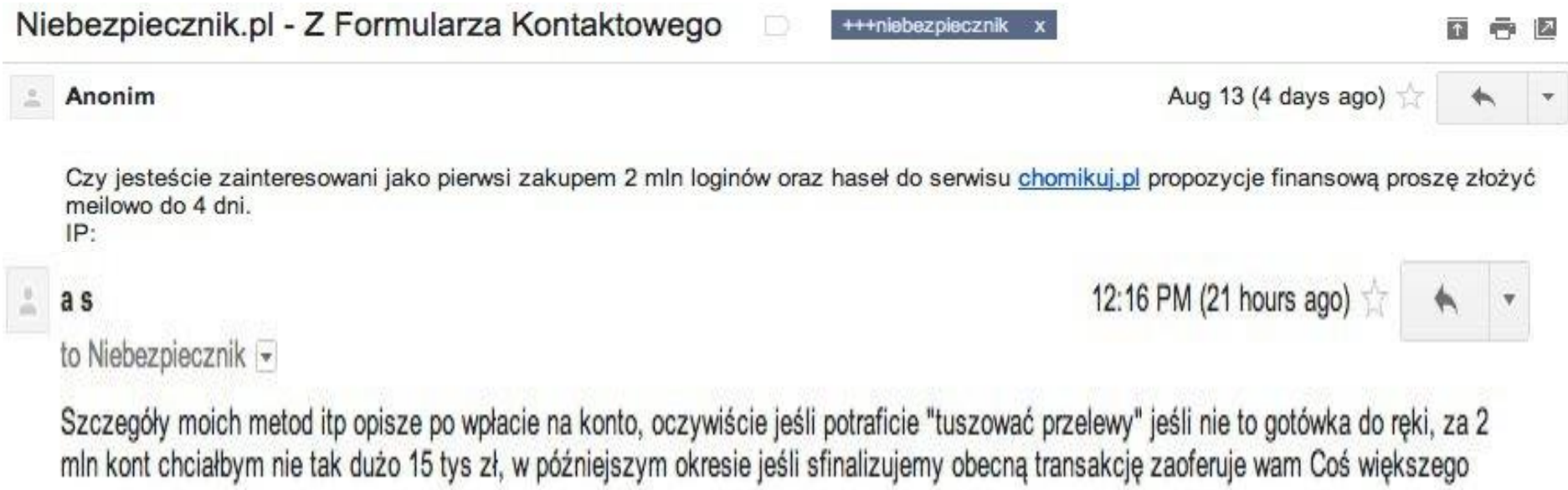
EnCase Forensic 7 umożliwia akwizycję danych z szerokiej gamy urządzeń cyfrowych, wskazanie dowodów i poszlak, a także tworzenie kompleksowych raportów z prowadzonych działań. Wszystko przy zachowaniu wartości dowodowej i integralności pozyskanych informacji.

EnCase Forensic 7 pozwala zabezpieczać dane z dysków, pamięci RAM, macierzy RAID, stacji roboczych, serwerów oraz smartfonów i tabletów, wraz ze znajdującymi się na nich: dokumentami plikami graficznymi, programami pocztowymi, webmail, artefaktami internetowymi, historią przeglądanych stron i pamięci podręcznej, rekonstrukcję strony HTML, czatów internetowych, plików skompresowanych, kopii bezpieczeństwa, plików zaszyfrowanych.

Przykład programu Encase (informatyka śledcza)



Sprzedaż danych – w tym rynek podziemny (darknet / deep web)


Niebezpiecznik.pl - Z Formularza Kontaktowego

+++niebezpiecznik x

Anonim Aug 13 (4 days ago)

Czy jesteście zainteresowani jako pierwsi zakupem 2 mln loginów oraz haseł do serwisu chomikuj.pl propozycje finansową proszę złożyć meilowo do 4 dni.
IP:

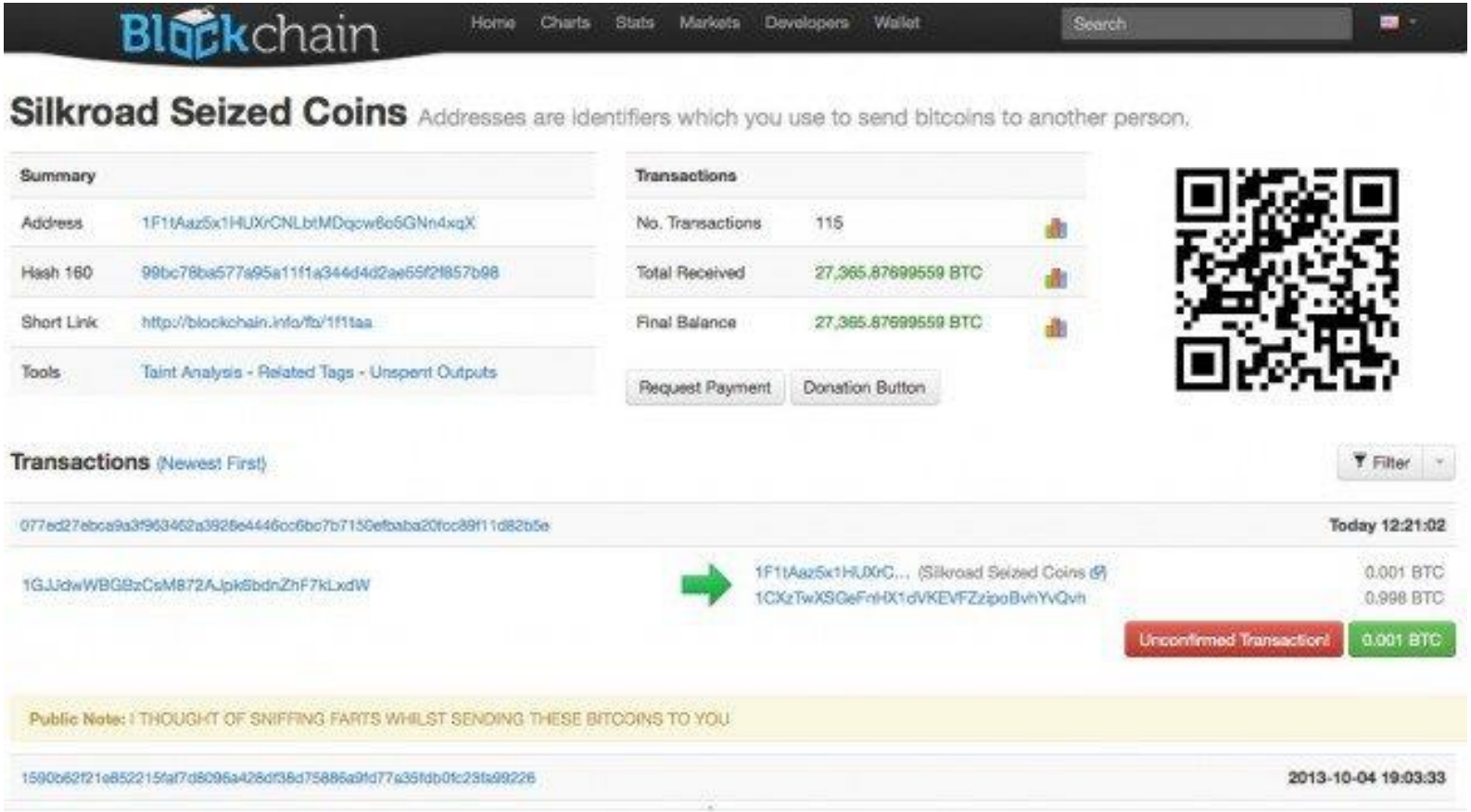
a s 12:16 PM (21 hours ago)

to Niebezpiecznik

Szczegóły moich metod itp opisze po wpłacie na konto, oczywiście jeśli potraficie "tuszować przelewy" jeśli nie to gotówka do ręki, za 2 mln kont chciałbym nie tak dużo 15 tys zł, w późniejszym okresie jeśli sfinalizujemy obecną transakcję zaoferuje wam Coś większego

http://niebezpiecznik.pl/post/chomikuj-pl-prosi-o-zmiane-hasla-dlaczego/?similarpostY6278x0

Sprzedaż Bitcoinów – w tym rynek podziemny (darknet / deep web)



Projekt Badawczo- Rozwojowy realizowany na rzecz bezpieczeństwa i obronności Państwa współfinansowany ze środków Narodowego Centrum Badań i Rozwoju
„MODEL REGULACJI JAWNOŚCI I JEJ OGRANICZEŃ W DEMOKRATYCZNYM PAŃSTWIE PRAWNYM”

Szpieg sprzedał w internecie aparat z tajnymi danymi

Dominik Błaszczykiewicz
PCWorld.pl

30.09.2008, godz. 12:40 | AAA

Bulwarowy dziennik brytyjski "The Sun" doniósł dziś o intrygującym skandalu związanym z brytyjskimi służbami wywiadowczymi. Według reporterów, jeden ze szpiegów organizacji MI6 sprzedał na aukcji internetowej aparat, na którym znajdowały się tajne dane związane z Al-Kaidą.

"The Sun" twierdzi, że jeden ze szpiegów brytyjskiego wywiadu sprzedał na aukcji internetowej aparat cyfrowy, na którym znajdowały się tajne dane związane z terrorystyczną Al-Kaidą. Agent przeoczył fakt, że w pamięci aparatu znajdowały się zdjęcia z nazwiskami działaczy Al-Kaidy, odciskami palców wraz z dokumentacją, a także fotografie broni przeciwpancernej.

Całość została sprzedana w sieci za jedyne 17 funtów. Osoba, która zakupiła sprzęt, natychmiast oddała go na komisariat policji. MI6 toczy w tej sprawie śledztwo.

http://www.pcworld.pl/news/168749/Szpieg.sprzedal.w.internecie.aparat.z.tajnymi.danymi.html

Projekt Badawczo- Rozwojowy realizowany na rzecz bezpieczeństwa i obronności Państwa współfinansowany ze środków Narodowego Centrum Badań i Rozwoju
„MODEL REGULACJI JAWNOŚCI I JEJ OGRANICZEŃ W DEMOKRATYCZNYM PAŃSTWIE PRAWNYM”

Facebook: DEA musi przestać tworzyć na portalu fikcyjne konta

Facebook zażądał od amerykańskiej agencji antynarkotykowej DEA gwarancji, że przestanie tworzyć na tym portalu fałszywe konta, by wykorzystywać je w prowadzonych dochodzeniach.

Specjalista Facebooka ds. bezpieczeństwa Joe Sullivan w liście skierowanym do szefowej DEA Michele Leonhart podkreślił, że korzystając z portalu, rządowe agencje muszą stosować się do tych samych zasad co zwykli użytkownicy, a więc powinny respektować m.in. zakaz podszywania się pod inne osoby.

To reakcja na pozew, jaki mieszkanka Nowego Jorku Sondra Arquiett wniosła wcześniej przeciw DEA. Kobieta twierdzi, że agent DEA stworzył w Internecie konto fikcyjnej osoby, używając w tym celu zdjęć z jej telefonu, by kontaktować się z "niebezpiecznymi osobnikami, w sprawie których prowadził śledztwo". Według Arquiett zdjęcia zostały zgrane z jej telefonu skonfiskowanego w 2010 r., gdy została zatrzymana za posiadanie narkotyków.

Facebook: DEA musi przestać tworzyć na portalu fikcyjne konta

Sullivan w liście napisał, że postępowanie DEA to "świadome i poważne naruszenie regulaminu Facebooka" oraz zażądał od rządowej agencji oświadczenia, że przestanie korzystać z fikcyjnych profili.

Ministerstwo sprawiedliwości początkowo broniło podobnych praktyk, twierdząc, że choć **Arquiett nie pozwoliła jednoznacznie agentowi na stworzenie fikcyjnego profilu** z jej zdjęciami, **to "pośrednio wyraziła na to zgodę, udostępniając dane ze swojego telefonu i zgadzając się, by zostały wykorzystane jako pomoc w prowadzonych dochodzeniach".** W ubiegłym tygodniu DEA ogłosiła, że sprawdzi, czy w sprawie fałszywego konta jej agent nie posunął się za daleko.

http://wiadomosci.wp.pl/kat,8311,title,Facebook-DEA-musi-przestac-tworzyc-na-portalu-fikcyjne-konta,wid,16968089,wiadomosc.html

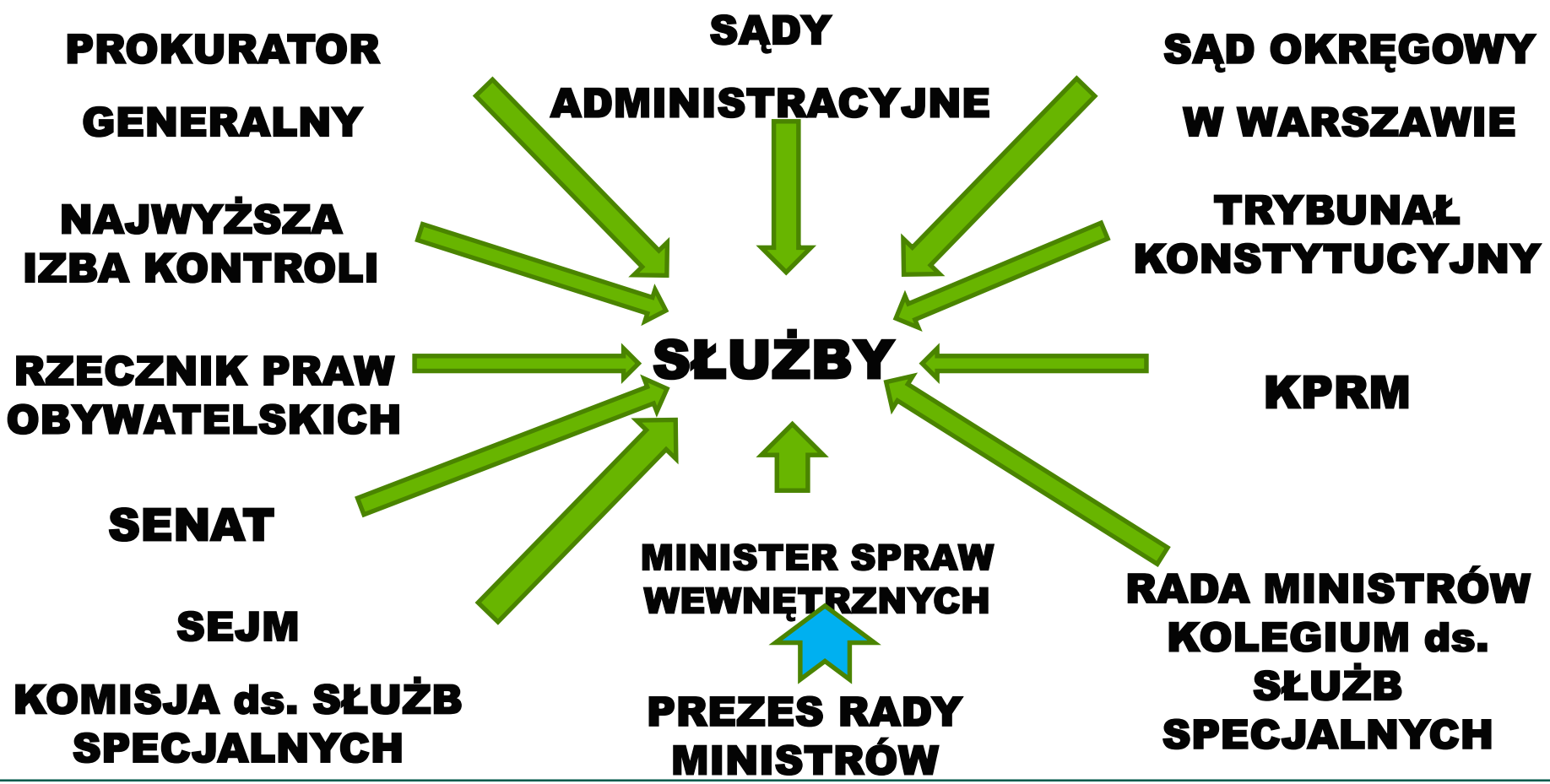
Kalejdoskop (z Niebezpiecznik.pl)

- Polska policja 86 razy poprosiła Google o szczegółowe dane internautów
- Twitter przekazał dane służbom
- Niemiecka policja szuka programisty do rządowego trojana
- CBŚ ujęło 17-letniego „cyberterrorystę” pomimo korzystania przez niego z TOR-a
- Polska w TOP10 krajów… proszących Google o dane użytkowników
- Dokumenty kapitana ABW w sieci TOR wykradzione z serwera FTP
- Czy polskie służby korzystają z włoskiego trojana tworzonego dla agencji rządowych?

Kalejdoskop (z Niebezpiecznik.pl)

- Czym rząd (brytyjski) hackuje telefony obywateli? – aplikacja może:
  * włączać mikrofon i podsłuchiwać otoczenie
  * podglądać otoczenie przez aktywację kamerki
  * podsłuchiwać odbierane wiadomości SMS i e-mail
  * ściągać zawartość książki kontaktowej
  * pobierać historię wykonanych połączeń
  * robić screenshoty tego co na ekranie
  * aktywować keyloggera
  * pobierać dane z GPS aby śledzić lokalizację

Kontrola i nadzór nas służbami ochrony państwa



Projekt Badawczo- Rozwojowy realizowany na rzecz bezpieczeństwa i obronności Państwa współfinansowany ze środków Narodowego Centrum Badań i Rozwoju
„MODEL REGULACJI JAWNOŚCI I JEJ OGRANICZEŃ W DEMOKRATYCZNYM PAŃSTWIE PRAWNYM”

Informacja o wynikach kontroli NIK kpb-p/12/191 (2 czerwca 2013)

Najwyższa Izba Kontroli ocenia **pozytywnie, pomimo stwierdzonych nieprawidłowości**, działalność kontrolowanych organów, służb i formacji w zakresie uzyskiwania i przetwarzania przez nie danych z bilingów, informacji o lokalizacji oraz innych danych, o których mowa w art. 180c i d ustawy Prawo telekomunikacyjne. W ocenie NIK, system pozyskiwania i przetwarzania ww. danych zapewniał realizację ustawowych zadań przez kontrolowane podmioty. **Wprowadzone zasady i procedury umożliwiały szybkie i sprawne pozyskiwanie danych w związku z prowadzonymi postępowaniami**. Możliwość sięgania **po dane telekomunikacyjne mieli jedynie upoważnieni pracownicy i funkcjonariusze**, a krąg osób posiadających takie upoważnienie był w kontrolowanych instytucjach ściśle określony.

Projekt Badawczo- Rozwojowy realizowany na rzecz bezpieczeństwa i obronności Państwa współfinansowany ze środków Narodowego Centrum Badań i Rozwoju
„MODEL REGULACJI JAWNOŚCI I JEJ OGRANICZEŃ W DEMOKRATYCZNYM PAŃSTWIE PRAWNYM”

Informacja o wynikach kontroli NIK kpb-p/12/191 (2 czerwca 2013)

Uwagi dotyczące kontrolowanej działalności	W ocenie NIK, brak rejestru osób upoważnionych do pozyskiwania danych telekomunikacyjnych za pośrednictwem sieci może utrudniać sprawowanie nadzoru nad prawidłowością działań funkcjonariuszy w tym zakresie. Badanie losowo wybranej próby dokumentów/zapisów dotyczących żądania udostępnienia danych telekomunikacyjnych wykazało uchybienia w zakresie upoważnienia funkcjonariuszy do przetwarzania danych osobowych w systemie *POEZJA* w ZSW oraz brak właściwego nadzoru ze strony Dyrektora ZSW.

Informacja o wynikach kontroli NIK kpb-p/12/191 (2 czerwca 2013)

Stwierdzone nieprawidłowości wiązały się m.in. z: przypadkami nieprzestrzegania obowiązujących przepisów, zasad i procedur oraz naruszenia tajemnicy telekomunikacyjnej; pozyskiwaniem danych za pośrednictwem sieci telekomunikacyjnej i systemów teleinformatycznych niespełniających wymagań technicznych i organizacyjnych; żądaniem udostępnienia danych telekomunikacyjnych za okres przekraczający 24 m-ce, **nieusuwaniem zbędnych danych telekomunikacyjnych**; brakiem właściwego nadzoru nad realizowanymi działaniami, w tym w szczególności nad przestrzeganiem przez przedsiębiorców telekomunikacyjnych obowiązków określonych w Prawie telekomunikacyjnym.

Informacja o wynikach kontroli NIK kpb-p/12/191 (2 czerwca 2013)

Opis stanu faktycznego	Dane telekomunikacyjne były kopiowane na zewnętrzne nośniki informacji w celu przeniesienia tych danych z komputera, z zainstalowanym systemem do prowadzenia zapytań u przedsiębiorcy, na komputer w sieci PSTD. Z-ca Dyrektora BK KGP wyjaśnił, że przenoszenie na nośnik odbywało się bez otwierania (analizowania) danych zawartych w pliku, a następnie plik trwale usuwano (kasowano) z pamięci poczty i dysków. Nieuprawnione kopiowanie, zostaje wyeliminowane z uwagi na dostęp do systemów tylko uprawnionych funkcjonariuszy, którzy mogą dokonać tego typu czynności. W przypadku nieprawidłowego działania w zakresie kopiowania – rozliczeniu podlega policjant otrzymujący dane i je wykorzystujący.

Informacja o wynikach kontroli NIK kpb-p/12/191 (2 czerwca 2013)

W ocenie NIK, obowiązujące przepisy w zakresie pozyskiwania przez uprawnione podmioty danych telekomunikacyjnych **nie chronią w stopniu wystarczającym praw i wolności obywatelskich przed nadmierną ingerencją ze strony państwa**. Niejednolitość i ogólnikowość przepisów uprawniających do pozyskiwania danych telekomunikacyjnych, może nasuwać wątpliwości, co do współmierności stosowanych ograniczeń praw i wolności obywatelskich w sferze wolności komunikacji z zasadami określonymi w Konstytucji RP.

Informacja o wynikach kontroli NIK kpb-p/12/191 (2 czerwca 2013)

Należy ponadto zauważyć, iż obowiązujący system zbierania informacji o zakresie wykorzystania przez organy państwa danych z bilingów, informacji o lokalizacji oraz innych danych, o których mowa w art. 180c i d ustawy Prawo telekomunikacyjne, **nie pozwala na określenie rzeczywistej liczby dokonywanych sprawdzeń**. Brak jest również mechanizmów kontroli o charakterze zewnętrznym, które pozwoliłyby na weryfikację zakresu wykorzystywania danych telekomunikacyjnych przez uprawnione podmioty, a w szczególności zasadności ich pozyskiwania i przetwarzania.

Projekt Badawczo- Rozwojowy realizowany na rzecz bezpieczeństwa i obronności Państwa współfinansowany ze środków Narodowego Centrum Badań i Rozwoju
„MODEL REGULACJI JAWNOŚCI I JEJ OGRANICZEŃ W DEMOKRATYCZNYM PAŃSTWIE PRAWNYM”

Informacja o wynikach kontroli NIK kpb-p/12/191 (2 czerwca 2013)

Uchybienia dotyczyły: braku skutecznej reakcji ABW na fakt otrzymywania od operatorów danych telekomunikacyjnych w szerszym zakresie, niż wynikało to ze stosownego zapytania

Szef CBA nie dysponował pełnym zakresem informacji, które umożliwiłyby sprawowanie rzetelnego nadzoru nad pozyskiwaniem danych telekomunikacyjnych w przypadku zapytań kierowanych za pomocą systemów teleinformatycznych

Projekt Badawczo- Rozwojowy realizowany na rzecz bezpieczeństwa i obronności Państwa współfinansowany ze środków Narodowego Centrum Badań i Rozwoju
„MODEL REGULACJI JAWNOŚCI I JEJ OGRANICZEŃ W DEMOKRATYCZNYM PAŃSTWIE PRAWNYM”

Informacja o wynikach kontroli NIK kpb-p/12/191 (2 czerwca 2013)

W ocenie NIK, obowiązujące przepisy w zakresie pozyskiwania przez uprawnione podmioty danych telekomunikacyjnych nie chronią w stopniu wystarczającym praw i wolności obywatelskich przed nadmierną ingerencją ze strony państwa. Biorąc pod uwagę istniejące uwarunkowania prawno-organizacyjne, projektowane zmiany przepisów na poziomie UE, a także wyniki przeprowadzonej kontroli, należy rozważyć podjęcie działań w **czterech** zasadniczych obszarach: zakresu i celu pozyskiwania danych; kontroli nad procesem pozyskiwania danych; niszczenia pozyskanych danych w sytuacji, gdy nie są już one dalej niezbędne dla osiągnięcia celów prowadzonego postępowania; stworzenia mechanizmów sprawozdawczych, które zapewnią rzetelną informację o zakresie pozyskiwania danych telekomunikacyjnych.

KONIEC

Dziękuję za uwagę

Projekt Badawczo- Rozwojowy realizowany na rzecz bezpieczeństwa i obronności Państwa współfinansowany ze środków Narodowego Centrum Badań i Rozwoju
„MODEL REGULACJI JAWNOŚCI I JEJ OGRANICZEŃ W DEMOKRATYCZNYM PAŃSTWIE PRAWNYM”