MAGAZYN

NR 21/MARZEC 2014

www.mediarecovery.pl/magazyn

INFORMATYKI ŚLEDCZEJ I BEZPIECZEŃSTWA IT

MobileIron (Mobile Device Management)

– czyli efektywne zarządzanie urządzeniami mobilnymi w firmie

Adrian Wróbel, Leszek Twardowski

Bring Your Own Device (BYOD)

– aspekty prawne

Jarosław Góra

Analiza urządzeń mobilnych

w oparciu o informatykę śledczą (mobile forensic)

Michał Tatar

Prepaid NIE ZAWSZE bezpieczny

Mateusz Witański

Prognozy dla rynku urządzeń mobilnych w Polsce

Damian Kowalczyk

Roztrzygnięcie konkursu „Ekspert informatyki śledczej" na stronie 2.

Od redakcji

Wykorzystanie w organizacjach rozwiązań do zarządzania urządzeniami mobilnymi – Mobile Device Management (MDM) przynosi konkretne korzyści biznesowe, przede wszystkim finansowe. To tylko jeden z powodów dla których coraz więcej menadżerów decyduje się na wdrożenie w ich organizacjach tego typu rozwiązania.

Dla wielu decydentów, rozwiązania do zarządzania urządzeniami mobilnymi, stają się elementem skutecznie budującym przewagę konkurencyjną ich przedsiębiorstwa. Takie podejście podyktowane jest coraz większą mobilnością pracowników.

Wielu ekspertów przewiduje że ten rok może okazać się przełomowy jeśli chodzi o ilość wdrożeń rozwiązań MDM. Wpływ na takie prognozy ma stale rosnący rynek urządzeń mobilnych w Polsce, jak również wdrażanie z sukcesem w wielu organizacjach podejścia Bring Your Own Device (BYOD), czyli wykorzystywania prywatnych smartfonów czy tabletów w celach służbowych.

Wierzymy, że po lekturze najnowszego Magazynu, wielu z Państwa lepiej zrozumie jak rozwiązania do zarządzania urządzeniami mobilnymi mogą zwiększyć potencjał biznesowy ich firm i organizacji.

Redakcja

Konkurs

Ekspert informatyki śledczej

Dziękujemy wszystkim uczestnikom za przesłane prace konkursowe. Konkurs uświadomił nam jak wielu spośród czytelników Magazynu Informatyki Śledczej i Bezpieczeństwa IT, interesuje się zawodowo oraz hobbystycznie zagnieniami w zakresie informatyki śledczej.

Lista zwycięzców konkursu

Wyróżnienie otrzymują Panowie: **Jacek Aniołek i Przemysław Cybulski,** którzy otrzymują gry logiczne Mediarecovery.

Prace konkursowe dostępne są na stronie: www.konkurs.mediarecovery.pl

MobileIron (Mobile Device Management)

- czyli efektywne zarządzanie urządzeniami mobilnymi w firmie

Adrian Wróbel, Leszek Twardowski

Globalny rynek urządzeń mobilnych przeżywa w ostatnich latach ogromny rozkwit. Statystyki pokazują, że obecnie mamy ponad 2 mld urządzeń na świecie. W przeciągu kolejnych 2 lat szacuje się, że ta liczba ma wzrosnąć o 30-40%. Oznacza to, że w 2016 roku co druga osoba będzie korzystała z urządzeń mobilnych. W skali globalnej są to ogromne ilości urządzeń, które wykorzystywane są zarówno do celów prywatnych, jak i zawodowych. Przetwarzamy na nich poufne dane logując się do portali społecznościowych, kont bankowych czy skrzynki e-mail. Dokonujemy zakupów, przeglądamy strony www, robimy zdjęcia, nagrywamy filmy, piszemy wiadomości, wysyłamy różne treści za pomocą komunikatorów. W ostateczności dzwonimy. Smartfony czy tablety stały się naszym mobilnym centrum nie tylko rozrywki, ale i informacji. Z poziomu jednego urządzenia mamy wygodny dostęp do niemalże wszystkiego. Tym samym nie zabezpieczając odpowiednio urządzenia narażamy się na nie tylko utratę danych, ale też przekazanie dostępu do nich osobom trzecim.

Obecnie mamy ponad 2 mld urządzeń na świecie. w 2016 roku co druga osoba będzie korzystała z urządzeń mobilnych.

Utrata zapisanych na urządzeniu danych może być więc dla nas katastrofalna w skutkach. O ile w przypadku prywatnych danych narażamy na poważną szkodę tylko siebie, o tyle przetwarzając służbowe dane na ich utracie może stracić cała firma. Korzystając z poczty e-mail mamy dostęp nie tylko do wiadomości, ale również do załączników. W pamięci urządzenia przechowujemy dokumenty w tym dane klientów czy umowy. Wydostanie się tych informacji poza nasze urządzenie może skutkować poważnymi konsekwencjami, w tym również finansowymi np. z tytułu kar za udostępnienie treści umowy.

Dużym wyzwaniem związanym z bezpieczeństwem danych jest trend nazwany BYOD (Bring Your Own Device) czyli udostępnianie na prywatnych urządzeniach mobilnych pracowników służbowych danych. Jest to zjawisko globalne. Co więcej wg. badań ok. 90% działów IT akceptuje BYOD, a ponad 60% jest przekonana do jego słuszności. Nie ma oczywiście w tym niczego złego, pod warunkiem odpowiedniego zabezpieczenia komunikacji i danych na takim urządzeniu oraz przeszkoleniu pracowników, w zakresie zagrożeń jakie mogą ich spotkać. W dobie rosnącej ilości urządzeń mobilnych, jak i BYOD niemal koniecznością jest wykorzystanie odpowiednich rozwiązań, które pozwolą nie tylko zarządzać całą flotą urządzeń mobilnych, ale również odpowiednio zabezpieczenie zapisanych na nich danych. Coraz więcej obok rozwiązań klasy MDM (Mobile Device Management) mówi się o konieczności stosowania systemów MAM (Mobile Application Management) czy też MCM (Mobile Content Management), które składają się na podejście nazywane Mobile IT.

W kompleksowym ujęciu problematyki oraz rosnącej skali urządzeń mobilnych niezbędne wręcz staje się zastosowanie technologii informatycznych. Niekwestionowanym liderem w obszarze MDM również w Polsce jest MobileIron. Rozwiązanie nie tylko całkowicie wspiera BYOD, ale również realizuje wielopoziomowe bezpieczeństwo zarówno poprzez szyfrowanie zapisanych danych w pamięci, szyfrowanie komunikacji aplikacji z serwerem czy też możliwość zablokowania lub wymuszenia konkretnych działań w obrębie konkretnych dokumentów. W przypadku kradzieży lub zgubienia urządzenia dane są całkowicie bezpieczne.

MobileIron gwarantuje wysoki poziom bezpieczeństwa oraz optymalne zarządzanie aplikacjami w ramach środowiska Enterprise.

Platforma jest wysoce skalowalnym rozwiązaniem, dostępnym w formie „On-Premise" lub „Cloud" (rozwiązanie w chmurze), które zostało od podstaw stworzone w celu ochrony i zarządzania mobilnymi aplikacjami, dokumentami oraz urządzeniami. Architektura MobileIron posiada trzy główne komponenty: 1. Usługi użytkownika końcowego dedykowane do zabezpieczania oraz zarządzania pocztą korporacyjną, aplikacjami, dokumentami oraz przeglądaniem stron internetowych. Te usługi są bezpośrednio dostępne dla użytkowników z ich urządzeń. MobileIron zapewnia dostarczenie, konfigurację oraz ochronę danych w spoczynku (data-at-rest). 2. Inteligenta brama (MobileIron Sentry) wykorzystywana do ochrony i zarządzania dostępem do zasobów korporacyjnych - bezpiecznie tuneluje ruch od użytkownika końcowego do zasobów firmowych takich jak np. Exchange, serwery aplikacji czy web, SharePoint. Odpowiada za ochronę danych w ruchu (data-in-motion). 3. Silnik konfiguracji polityk oraz profili pozwala globalnie zarządzać aplikacjami, dokumentami oraz urządzeniami. Ten komponent nosi nazwę MobileIron VSP (dla instalacji On-premise) oraz MobileIron Connected Cloud dla instalacji w chmurze.

W ten sposób zaprojektowana platforma MobileIron gwarantuje wysoki poziom bezpieczeństwa oraz optymalne zarządzanie aplikacjami w ramach środowiska Enterprise. Najważniejszymi korzyściami jakie oferuje MobileIron dla globalnych organizacji, średnich i małych firm są m.in.: wsparcie dla różnych systemów mobilnych, rozwiązanie Data Loss Prevention (DLP) dla natywnej poczty email, ochronę prywatności oraz separację danych, bezpieczeństwo poprzez wykorzystanie certyfikatów dla użytkownika, konfigurację Multi-user dla współdzielonych urządzeń. MobileIron według badań firmy Gartner jest światowym liderem w dziedzinie ochrony i zarządzania urządzeniami mobilnymi. Rozwiązanie spełnia również wymagania międzynarodowej normy bezpieczeństwa ISO 27001: A.11.7.

Adrian Wróbel – autor jest konsultantem ds. bezpieczeństwa w firmie Mediarecovery.

Leszek Twardowski – autor jest konsultantem ds. bezpieczeństwa w firmie headtechnology.

MOBILE DEVICE **MANAGEMENT**

Bring Your Own Device (BYOD) – aspekty prawne

Jarosław Góra

BYOD, czyli Bring Your Own Device to coraz bardziej popularne zjawisko wykorzystywania prywatnych urządzeń do celów służbowych. Wykonując obowiązki służbowe pracownicy często korzystają z własnych telefonów, komputerów i innego sprzętu elektronicznego, z którym najczęściej związane jest oprogramowanie (od systemu operacyjnego do poszczególnych programów komputerowych). Co więcej, nawet jeśli pracodawca dostarcza odpowiedni sprzęt pracownicy często korzystają z prywatnego, np. kiedy „zabierają prace do domu". Wdrażając rozwiązania BYOD pracodawcy dbają najczęściej o kwestie związane z bezpieczeństwem informacji przetwarzanych za pomocą prywatnego sprzętu, ale często zapominają o aspektach prawnych z tym związanych.

Prawne problemy z BYOD ujawniają się w kilku obszarach. Punktem wyjścia powinna być odpowiedź na pytanie, czy prawo, a przede wszystkim prawo pracy, w ogóle dopuszcza takie rozwiązanie? W kodeksie pracy, jak i innych aktach regulujących tą dziedzinę prawa (oprócz przepisów dotyczących korzystania z samochodu prywatnego do celów służbowych), nie znajdziemy regulacji bezpośrednio dotykających BYOD. Zgodnie jednak z podstawową zasadą prawa pracy i art. 94 kodeksu pracy dostarczanie narzędzi pracy jest jednym z podstawowych obowiązków pracodawcy. Czy można przerzucić ten obowiązek na pracownika? W art. art. 6711 § 2 kodeksu pracy przeczytamy, że pracodawca i telepracownik mogą, w odrębnej umowie, określić w szczególności zakres ubezpieczenia i zasady wykorzystywania przez telepracownika sprzętu niezbędnego do wykonywania pracy w formie telepracy, stanowiącego własność telepracownika. Rozwiązanie to dotyczy telepracownika, jednak mając również na uwadze dopuszczalne prawem wykorzystywanie samochodu prywatnego do celów służbowych, pozwala nam to wysunąć wniosek, iż prawo pracy nie zakazuje uregulowania kwestii BYOD w porozumieniu z pracownikiem. Stanowisko to zostało potwierdzone również w orzecznictwie (patrz wyrok SN z dnia 25.11.04 r., I PK 42/04; wyrok SN z dnia 12.03.09 r., II PK 198/08).

Jak zatem wdrożyć model BYOD? Czy rozwiązanie takie można narzucić pracownikom, czy też niezbędne jest uzyskanie ich zgody? Od razu wskazać należy, że narzucenie takiego rozwiązania nie wchodzi w grę, bowiem stoi w sprzeczności z podstawową zasadą prawa pracy i obowiązkiem pracodawcy do organizacji pracy i dostarczenia odpowiednich narzędzi. W grę wchodzi zatem jedynie porozumienie z pracownikami. Czy jednak zgoda na wdrożenie rozwiązania BYOD będzie skuteczna?

Naczelny Sąd Administracyjny kilkukrotnie wskazywał, że problematyka zgody w stosunkach pracowniczych jest kontrowersyjna i może być kwestionowana jako wymuszona (patrz wyrok NSA z dnia 01.12.2009 r., I OSK 249/09). Pamiętać zatem należy, aby pracownikowi stworzyć rzeczywiste warunki do dobrowolnego skorzystania z modelu BYOD, wtedy takie działanie będzie dopuszczalne. Musi zatem istnieć alternatywa. Prywatny sprzęt pracownika wykorzystywany w pracy zostaje objęty firmowym systemem bezpieczeństwa i powinien spełniać wszystkie przewidziane w nim wymagania. Jednym z elementów każdego systemu bezpieczeństwa jest możliwość sprawowania kontroli. Czy pracodawca jest uprawniony do wykonywania kontroli w zakresie prywatnego sprzętu pracownika? Czy po ustaniu stosunku pracy pracownik będzie zobligowany do „zwrotu" lub wykasowania wszelkich służbowych materiałów (informacji) z prywatnego sprzętu i czy pracodawca będzie w jakiś sposób uprawniony do zweryfikowania wykonania tego obowiązku?

Brak powszechnie obowiązujących regulacji prawnych w tym zakresie wymusza wewnętrzne uregulowanie tych kwestii, w regulaminach, politykach lub dodatkowych porozumieniach z pracownikami, mając na uwadze wszelkie kontrowersje związane z kontrolą pracowników, takie jak prawo do prywatności (jasne reguły, transparentność itp.).

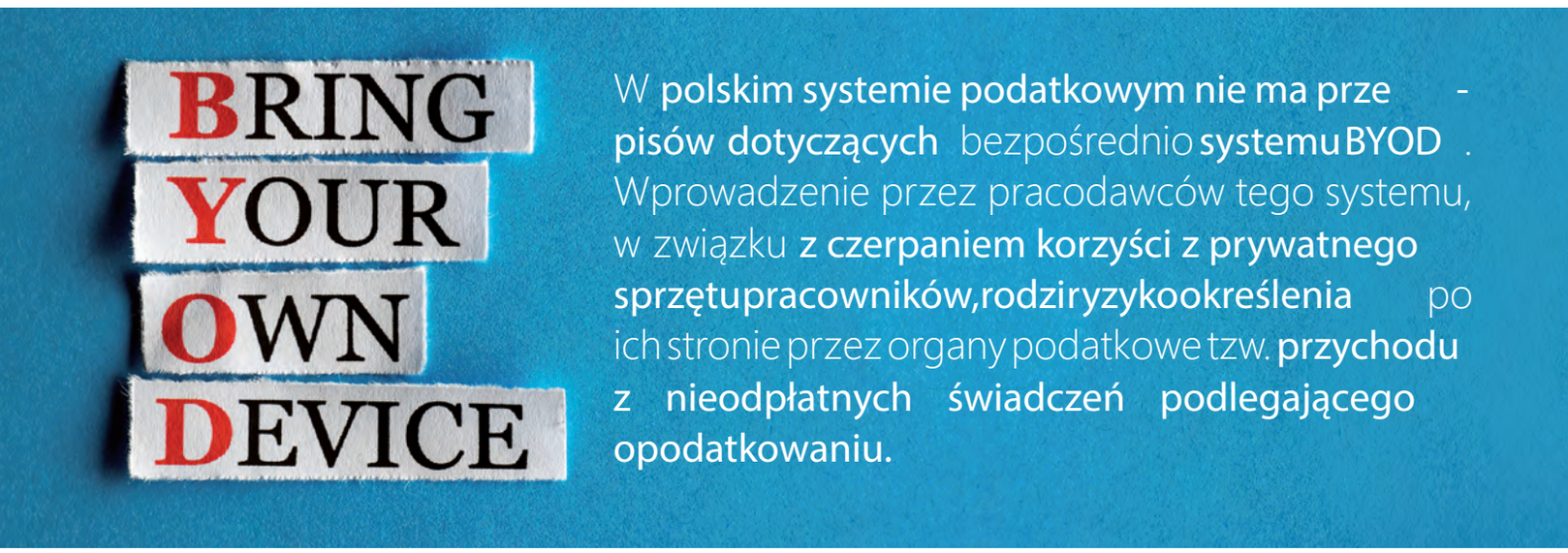
Ze sprzętem elektronicznym takim jak laptopy, czy też prywatne komputery stacjonarne najczęściej związane

Prywatny sprzęt pracownika wykorzystywany w pracy zostaje objęty firmowym systemem bezpieczeństwa i powinien spełniać wszystkie przewidziane w nim wymagania.

jest jakiegoś rodzaju oprogramowanie. Mam tutaj na myśli zarówno system operacyjny, jak i poszczególne programy komputerowe wykorzystywane do wykonywania obowiązków pracowniczych. Czy licencje posiadane przez pracowników pozwalają na wykorzystywanie oprogramowania w celach służbowych? Na posiadanym przez pracowników prywatnym sprzęcie komputerowym zainstalowany jest najczęściej system operacyjny w wersji „home edition" lub inny podobny. Tego rodzaju licencja upoważnia do korzystania z oprogramowania jedynie w celach prywatnych (non-commercial use). Podobna sytuacja może mieć miejsce w przypadku pozostałego oprogramowania, np. graficznego. W takim wypadku wykorzystanie prywatnego sprzętu i oprogramowania na nim zainstalowanego w celach służbowych może stanowić naruszenie licencji. Rozwiązaniem takiego problemy będzie wyposażenie pracownika przez pracodawcę w odpowiednie oprogramowanie, którego licencja upoważnia do wykorzystywania go w celach komercyjnych.

Na sprzęcie pracownika można zainstalować osobny system operacyjny, założyć odrębne konto użytkownika i zainstalować odpowiednie oprogramowanie. W życiu pewne są tylko dwie rzeczy... W przypadku BYOD natomiast często nie myśli się o drugiej z tych rzeczy, czyli podatkach. W polskim systemie podatkowym nie ma przepisów dotyczących bezpośrednio systemu BYOD. Wprowadzenie przez pracodawców systemu BYOD, w związku z czerpaniem korzyści z prywatnego sprzętu pracowników, rodzi ryzyko określenia po ich stronie przez organy podatkowe tzw. przychodu z nieodpłatnych świadczeń podlegającego opodatkowaniu. Zasadniczo bowiem, gdy podmiot prowadzący działalność gospodarczą otrzyma nieodpłatne świadczenie (lub świadczenie częściowo odpłatne) zobowiązany jest wykazać z tego tytułu przychód podatkowy. W ustawach podatkowych brak natomiast definicji nieodpłatnego świadczenia. Sądownictwo administracyjne wypracowało pogląd, że dla celów podatkowych nieodpłatnymi świadczeniami są wszelkie zjawiska gospodarcze i zdarzenia prawne, których następstwem jest uzyskanie korzyści kosztem innego podmiotu lub te wszystkie zdarzenia prawne i zdarzenia gospodarcze w działalności osób prawnych, których skutkiem jest nieodpłatne, tj. niezwiązane z kosztami lub inną formą ekwiwalentu, przysporzenie majątku tej osobie, mające konkretny wymiar finansowy. Dla pracodawców prowadzących jednoosobową działalność gospodarczą aktualny będzie oczywiście podatek PIT, natomiast dla osób prawnych podatek CIT. Jaka będzie wartość przychodów w przypadku BYOD? Jeżeli przedmiotem nieodpłatnego świadczenia jest rzecz lub prawo, wartość przychodu określa się na podstawie cen rynkowych stosowanych w obrocie rzeczami lub prawami tego samego rodzaju i gatunku, z uwzględnieniem w szczególności ich stanu i stopnia zużycia oraz czasu i miejsca ich uzyskania. Jak widać, oparcie się na obowiązujących przepisach, które nie dotykają bezpośrednio problematyki BYOD może rodzić szereg problemów natury praktycznej. Z tego też względu zaleca się, aby zabezpieczyć się przed ryzykiem ustalenia przez organy, że pracodawca otrzymuje nieodpłatne świadczenie w związku z wprowadzeniem systemu BYOD, wprowadzenie do umowy o pracę klauzuli dotyczącej ekwiwalentu pieniężnego za używanie przez pracownika przy wykonywaniu pracy jego własnego sprzętu. Problematyczną kwestią jest niestety nadal ustalenie wartości takiego ekwiwalentu, która powinna odpowiadać wartości zużycia sprzętu w trakcie jego wykorzystywania do celów służbowych. Wydaje się, że wartość taka powinna być ustalana z uwzględnieniem stopnia zużycia sprzętu i udokumentowanych cen rynkowych. Po stronie pracownika wypłata takiego

Zaleca się w związku z wprowadzeniem systemu BYOD, wprowadzenie do umowy o pracę klauzuli dotyczącej ekwiwalentu pieniężnego za używanie przez pracownika przy wykonywaniu pracy jego własnego sprzętu.

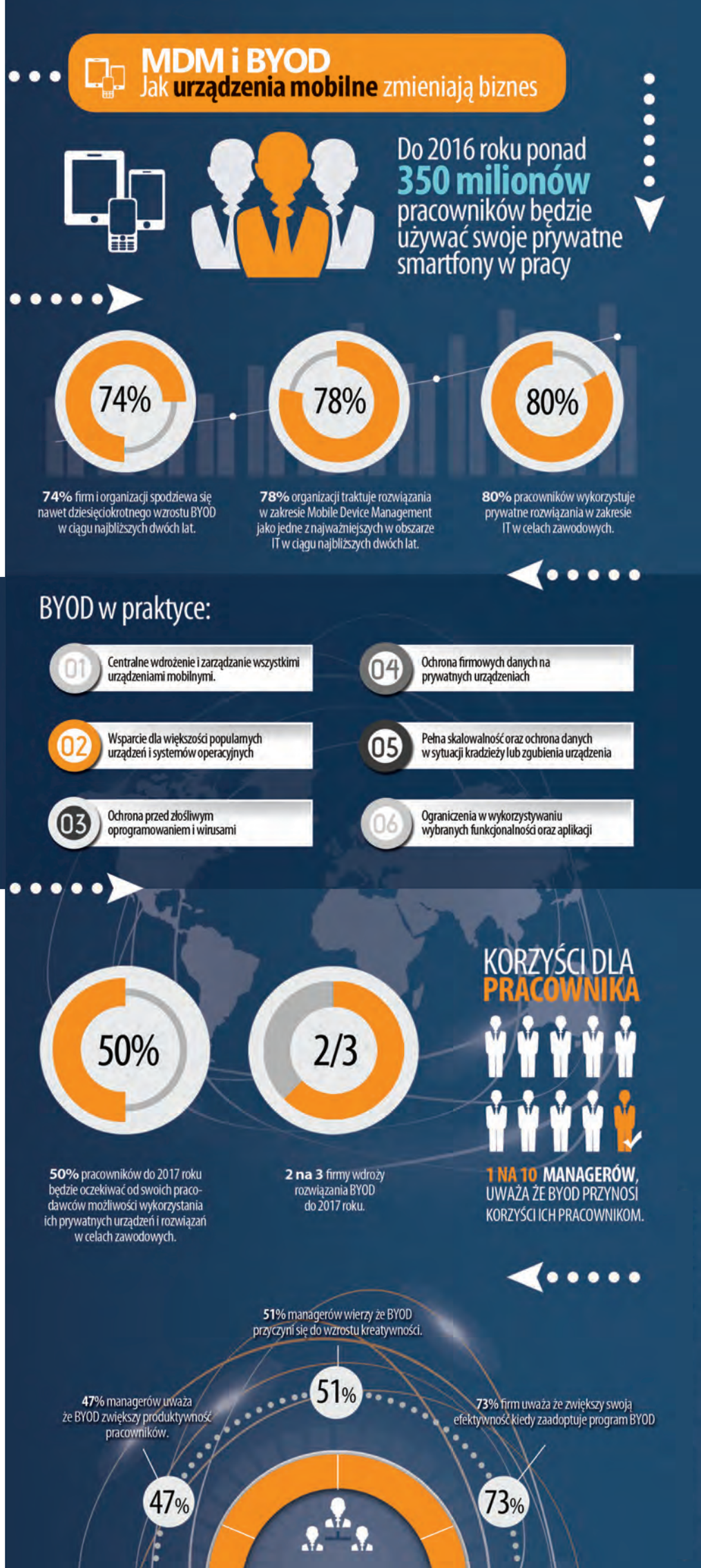


W polskim systemie podatkowym nie ma przepisów dotyczących bezpośrednio systemu BYOD. Wprowadzenie przez pracodawców tego systemu, w związku z czerpaniem korzyści z prywatnego sprzętu pracowników, rodzi ryzyko określenia po ich stronie przez organy podatkowe tzw. przychodu z nieodpłatnych świadczeń podlegającego opodatkowaniu.

ekwiwalentu nie będzie rodziła skutków podatkowych, ponieważ wypłacony pracownikowi ekwiwalent byłby wolny od podatku dochodowego na podstawie art. 21 ust. ustawy z dnia 26 lipca 1991 r. o podatku dochodowym od osób fizycznych. Natomiast po stronie pracodawcy brak przeszkód do zaliczenia tego ekwiwalentu do kosztów uzyskania przychodów. Model BYOD z impetem „wkroczył na salony" i jest wykorzystywany na rynku dość powszechnie. Firmy wdrażają to rozwiązanie w całości (pracownik korzysta tylko z własnego sprzętu) lub częściowo. Nie wszędzie natomiast pracodawcy decydują się na odpowiednie uregulowanie zasad funkcjonowania tego modelu, funkcjonując na zasadzie ustnego porozumienia z pracownikami i utartych praktyk, pozostawiając te kwestie jakby w „szarej strefie". Problemy pojawiają się oczywiście w przypadku nieprawidłowości wykrytych w trakcie kontroli, nieprawidłowości księgowo-podatkowych, czy też sporów z [byłymi]pracownikami. Warto zatem odpowiednio uregulować kwestie funkcjonowania BYOD, mając na uwadze zasygnalizowane wyżej aspekty prawne.

Model **BYOD** z impetem „wkroczył na salony" i **jest wykorzy - stywany** na rynku dość powszechnie.

Autor jest aplikantem adwokackim, szefem zespołu prawa własności intelektualnej i nowych technologii w kancelarii Ślązak, Zapiór i Wspólnicy. Trener w Akademii Informatyki Śledczej.



Analiza urządzeń mobilnych w oparciu o informatykę śledczą (mobile forensic)

Michał Tatar

W dzisiejszym cyfrowym i przede wszystkim mobilnym świecie nie sposób sobie wyobrazić sytuację, w której wychodząc z naszego domu nie trafimy na ludzi użytkujących telefon komórkowy. Jedni przez nie rozmawiają, inni robią właśnie jakieś zdjęcie, a jeszcze inni przeglądają Internet. Jak podaje Główny Urząd Statystyczny liczba abonentów telefonii komórkowej wyniosła na koniec 2013r. blisko 55 mln. To dwa razy więcej niż osiem lat temu. Dziś na każdego Polaka - dorosłego i dziecko, noworodka i starca - przypada 1,5 komórki. Na jedno gospodarstwo domowe - około czterech.

Skalę danych zawartych we wszystkich telefonach komórkowych ciężko oszacować, zwłaszcza w dobie gdzie telefony komórkowe posiadają spore magazyny pamięci jednak słowo 'ogrom' będzie na pewno adekwatne. Książki kontaktów, wiadomości SMS czy rejestry połączeń to tylko mała część tych informacji. Mając na uwadze jakże popularne w Polsce smartfony, tak naprawdę w pamięci urządzenia może znajdować się wszystko. Począwszy od zdjęć, plików muzycznych czy też wideo, dokumentów, poczty elektronicznej, a skończywszy na danych geolokalizacyjnych, nie wspominając już o plikach tymczasowych z przeglądania Internetu. W związku z powyższym możemy zadać sobie pytanie – jakie podejście w ramach informatyki śledczej należy zastosować?

> Według danych udostępnionych przez Policję, na koniec 2012 roku odnotowano ok. 46 tys. przestępstw, gdzie telefon komórkowy był głównym przedmiotem przestępstwa.

Czy zabezpieczenie tego typu urządzeń jest proste czy może jednak okazać się dla nas koszmarem? Niestety, odpowiedź nie jest jednoznaczna i mogę tutaj użyć mojego ulubionego, aczkolwiek nie pożądanego słowa – to zależy. Proces zabezpieczenia danych z telefonów komórkowych zależy przede wszystkim od urządzenia. Na naszym rodzimym rynku odnajdziemy najbardziej popularne modele telefonów, jak i te które dotarły do nas z odległych zakątków świata. W związku z tym nie należy przyjmować zabezpieczenia danych jako procedurę standardową stosowaną dla każdego urządzenia. Każdy telefon komórkowy powinien być dla nas nową sprawą i należy ją potraktować indywidualnie, mimo iż zabezpieczając tego rodzaju sprzęt możemy trafić po raz kolejny na takie same urządzenie. Dlaczego? Posłużę się przykładem z laboratorium Mediarecovery. Sprawa,

o której piszę wydawała się z pozoru prosta. Dostałem trzy takie same modele telefonów komórkowych firmy Sony Ericsson, które różniły się na pierwszy rzut oka tylko kolorem obudowy. Po szczegółowej analizie okazało się jednak, że na każdym z tych urządzeń zainstalowano inną wersję systemu operacyjnego. W związku z tym, mimo iż telefony zostały wyprodukowane przez tego samego producenta, mimo iż wyglądały tak samo i ich obsługa była taka sama należało każde z tych urządzeń odczytać w inny sposób. Wracając do kwestii zabezpieczenia danych z telefonów komórkowych powinniśmy rozumieć skalę wykorzystania tego rodzaju urządzeń w przestępstwach.

Według danych udostępnionych przez Policję, na koniec 2012 roku odnotowano ok. 46 tys. przestępstw, gdzie telefon komórkowy był głównym przedmiotem przestępstwa. Dodatkowo warto odnotować informacje odnośnie możliwości połączenia telefonu z Internetem i pobieraniu/wysyłaniu danych w sieci. W tej chwili średnia pobieranych danych przez telefon komórkowy na rynku światowym to 300-500 MB miesięcznie na użytkownika. Ale do 2020 r. wielkość ta powinna się znacząco zwiększyć i osiągnąć 1 GB dziennie na użytkownika.

Powyższe informacje dają jasny obraz tego z czym informatyk śledczy ma do czynienia. Jak zatem można poradzić sobie z tym wszystkim w miarę prosty sposób, który również zaoszczędzi nam sporą ilość czasu na ręcznym sprawdzaniu danych z telefonów komórkowych? Moją odpowiedzią na przedstawione pytanie jest oprogramowanie XRY. Poprzez narzędzie XRY informatyk śledczy dostaje kompleksowe narzędzie do zabezpieczeń danych z telefonów komórkowych, kart SIM czy kart pamięci. Za pomocą oprogramowania XRY możemy sklonować kartę SIM czy przeprowadzić fizyczną akwizycję pamięci w celu podjęcia próby odzyskiwania skasowanych danych. Dysponowanie jednak samym oprogramowaniem to oczywiście nie wszystko. Niestety telefon komórkowy jako dowód elektroniczny jest niewdzięcznym urządzeniem, gdyż nawet najmniejsza nieznajomość procedur i brak odpowiedniej wiedzy na temat tego co może naruszyć integralność pamięci, może wykluczyć telefon komórkowy jako dowód. Każdy popełniony błąd może być zaprzepaszczoną szansą na poprawną ekstrakcję danych. Dlatego spróbuję w kilku punktach opisać najlepsze praktyki informatyki śledczej w zabezpieczeniu tego rodzaju urządzeń, wykorzystując przy tym narzędzie XRY.

Średnia pobieranych danych przez telefon komórkowy na rynku światowym to 300-500 MB miesięcznie na użytkownika. do 2020 r. wielkość ta powinna się znacząco zwiększyć i osiągnąć 1 GB dziennie.

1) Zabezpieczony telefon komórkowy czy inne urządzenie mobilne powinno zostać dokładnie opisane. - Każde urządzenie posiada numer IMEI, który sprawdzić możemy poprzez wybranie na włączonym urządzeniu klawiszy *#06# lub jeśli urządzenie jest wyłączone staramy się zlokalizować numer IMEI na naklejce producenta. - Każda karta SIM posiada numer ICC, który najczęściej jest nadrukowany na kartę SIM i zaczyna się od numeru 89.

2) Staramy się pozyskać wszelkie możliwe kody zabezpieczające kartę SIM bądź samo urządzenie. O ile z niektórych zabezpieczonych urządzeń możemy za pomocą narzędzia XRY dostać się do pamięci telefonu, tak w przypadku kart SIM nie jest to w żaden sposób możliwe.

3) Nie mając przy sobie sprzętu do zabezpieczenia danych urządzenie najlepiej wyłączyć by nie dopuścić do sytuacji, że telefon pobiera nowe dane bądź też jest zdalnie zarządzany.

4) Najlepszą praktyką jest oddzielić telefon komórkowy od karty SIM by na wypadek przypadkowego włączenia urządzenie nie zalogowało się do sieci GSM.

5) Za pomocą oprogramowania XRY i dołączonego do niego Device Manual należy sprawdzić czy na zabezpieczonym telefonie komórkowym możemy wykonać akwizycję logiczną/fizyczną, jaki wybrać sposób komunikacji pomiędzy telefonem, a komputerem czy też jakim kablem należy się posłużyć. Możemy się także dowiedzieć czy telefon możemy odczytać bez karty SIM czy z nią.

6) Jeśli telefon komórkowy musimy odczytać z kartą SIM to NIGDY nie używamy do tego oryginalnej karty SIM. Oryginalną kartę SIM należy uprzednio sklonować i tylko na takiej karcie SIM wykonywać odczyt – sklonowana karta SIM to gwarancja, że telefon nie zaloguje się do sieci GSM.

7) Po pomyślnym odczycie pamięci telefonu/karty SIM pracujemy tylko i wyłącznie na plikach z odczytu.

Analiza urządzeń mobilnych w oparciu o informatykę śledczą posiada swoją odrębną specyfikę wynikającą z typów i rodzajów analizowanych telefonów, smartfonów czy tabletów, a jej rozwój jest wprost proporcjonalny do ilości urządzeń mobilnych na rynku. Należy jednak pamiętać, że za rozwojem tej dyscypliny stoją rozwiązania i najlepsze praktyki, mające swój początek w informatyce śledczej.

Autor jest specjalistą IT w laboratorium Mediarecovery.

MAGAZYN
INFORMATYKI ŚLEDCZEJ I BEZPIECZEŃSTWA IT

Adres redakcji
Mediarecovery
40-723 Katowice, ul. Piotrowicka 61
Tel. 32 782 95 95, fax 32 782 95 94
e-mail: redakcja@mediarecovery.pl

Redakcja
Sebastian Małycha (red. nacz.),
Przemysław Krejza
Skład, łamanie, grafika: Marcin Wojtera
Reklama: Damian Kowalczyk

Wydawca
Media Sp. z o.o.
40-723 Katowice, ul. Piotrowicka 61
Tel. 32 782 95 95, fax 32 782 95 94
e-mail: biuro@mediarecovery.pl

mediarecovery
Lider informatyki śledczej

Prepaid nie zawsze bezpieczny

Mateusz Witański

Zbigniew chciał zemścić się na swoim byłym pracodawcy. Postanowił postraszyć go w sprawie, o której wiedział on i kilku zaufanych pracowników. Aby nie wpaść, postanowił kupić kartę prepaid z przypadkowym numerem i wysłać kilka sms-ów, może raz czy dwa zadzwonić. Kilkanaście dni po rozstaniu z firmą zrealizował swój plan. Do swojego telefonu włożył kartę prepaid, dla upewnienia się, że nie identyfikuje się swoim numerem zadzwonił do najlepszego przyjaciela. Następnie przez kilka dni postępował zgodnie ze schematem – rano w pracy wysyłał kilka sms-ów o różnej treści do swoich przełożonych z poprzedniej firmy, następnie wieczorem ponownie wysyłał sms-y, tym razem do kadry zarządzającej z groźbami. Wszystkie sms-y w telefonie kasował zaraz po wysłaniu. Swój proceder uprawiał przez dwa tygodnie. Jakie było jego zdziwienie, gdy po kilku miesiącach zapukała do niego policja z nakazem zabezpieczenia jego telefonu oraz przeszukania mieszkania w celu znalezienia wszystkich kart SIM, jakie Zbigniew posiada.

W roku 2006 w monografii „Przestępstwa telekomunikacyjne" Maciej Rogalski wymienia m.in. następujące przestępstwa związane z telekomunikacją: przeciwko wiarygodności dokumentów, kradzieży aparatu telefonicznego, kradzieży impulsów telefonicznych, oszustwa usług telekomunikacyjnych. Obecnie o przestępstwach telekomunikacyjnych możemy mówić także w przypadku takich działań, jak: stalking, phishing, kradzież dóbr materialnych, kradzież tożsamości, molestowanie psychiczne i wiele innych. Z telekomunikacją wiąże się także przestępstwa gospodarcze i kryminalne.

Użytkownicy telefonów kupują karty prepaid, żeby wykonać połączenia głosowe czy sms-owe, których nie chcą mieć na rachunku i w billingu.

Wachlarz ten jest bardzo szeroki, a ilość przestępstw dokonywanych przy pomocy telefonu i wykrywanych przy udziale danych telekomunikacyjnych z każdym rokiem rośnie. Wzrasta więc świadomość przestępców i służb ścigania w aspekcie stosowanych metod popełniania przestępstw.

Jedną z takich metod jest korzystanie z kart SIM, które nie są rejestrowane, przez co są potencjalnie niewykrywalne. Stosunkowo często zdarza się, że użytkownicy telefonów kupują karty prepaid, żeby wykonać pewne połączenia głosowe czy sms-owe, których nie chcą mieć na rachunku i w billingu. Gdy wykorzystywane jest to do zakupu usług płatnych, , nie wydaje się to praktyką naganną. Można powiedzieć, że jest to bardzo pomysłowe i mało kłopotliwe. Wykorzystanie takiego numeru zabezpiecza nas zarówno przed przekroczeniem kosztów przeznaczonych na te usługi (karta prepaid ma określoną wartość, której przekroczyć nie można), jak i przed ewentualnymi reklamami dotyczącymi tych usług (nie zawsze chcemy ponownie korzystać z tego typu usług).

Zupełnie inaczej sprawa się przedstawia, gdy wykorzystujemy kartę prepaid do popełnienia przestępstwa, bez względu na jego charakter. W tym przypadku fakt korzystania z kart prepaid wynika tylko

i wyłącznie z chęci zatarcia śladów. Większość z nas nie ma świadomości, że w tej sytuacji istnieje bardzo duże prawdopodobieństwo wykrycia sprawcy przestępstwa. Skąd się bierze ta pewność wykrycia sprawcy, skoro korzysta z numeru prepaid, który można kupić obecnie w kiosku z gazetami? Oferta prepaid (sprzedaż przedpłacona) sieci telefonii komórkowych polega na zakupieniu przez klienta określonej liczby jednostek taryfikacyjnych. Opłata jest wnoszona z góry, natomiast wykorzystanie nabytych jednostek jest możliwe przez czas określony przez operatora. Po tym okresie konieczne jest ponowne uzupełnienie konta. Jednostki są odejmowane z konta użytkownika proporcjonalnie do wykonanych połączeń i wykorzystanych usług dodatkowych. Doładowanie konta i odnowienie limitu jednostek następuje po zakupie specjalnego kuponu.

Cechą charakterystyczną oferty prepaid jest brak konieczności zawarcia pisemnej umowy z operatorem, jest ona zawierana przez dokonanie czynności faktycznych. Tak więc sprzedaż przedpłacona daje nam gwarancję, że nie zostaniemy bezpośrednio połączeni z numerem prepaid. Daje nam więc pewną „gwarancję nietykalności". Gdy popełnimy błąd przy wykorzystaniu tej metody podczas przestępstwa, gwarancji takiej mieć nie będziemy. Bardzo wysokie prawdopodobieństwo wykrycia sprawcy przestępstwa bierze się stąd, że korzystamy z telefonów. Można założyć, że większość osób, które zakupi kartę prepaid, włoży ją do posiadanego telefonu, aby wykonać „bezpieczne" połączenie.

Karty prepaid na pewno nie zapewnią nam bezpieczeństwa w trakcie popełniania przestępstwa.

Naszej sytuacji nie polepszy nawet fakt włożenia karty do telefonu dawno nieużywanego. Większość z nas nie zdaje sobie bowiem sprawy, że każdy telefon identyfikuje się w sieci odpowiednim numerem IMEI, wskazującym jednoznacznie konkretny aparat telefoniczny. Dotarcie do tego, kto aktualnie używa danego aparatu nie nastręcza wielu trudności.

Dane telekomunikacyjne z karty prepaid jednoznacznie wskażą, z jakiego telefonu zostały wykonane połączenia lub wysłane sms-y. W kolejnych krokach możemy zidentyfikować jakie inne karty SIM korzystały z tego telefonu (prepaid i abonamentowe), do kogo należą te karty SIM (wraz z informacją, z jakich innych telefonów karty te korzystały), czy z tych kart SIM korzystano w momencie aktywności danej karty prepaid, można określić logowanie się kart SIM do BTS-ów (wraz z czasem aktywności i nieaktywności danej karty). Dodatkowo mając kartę prepaid oraz IMEI telefonu, możemy sprawdzić, gdzie i kiedy zostały zakupione, a w przypadku telefonu prześledzić jego historię. Danych do analizy jest więc mnóstwo, trzeba tylko wiedzieć, jak się wśród nich poruszać.

Karty prepaid na pewno nie zapewnią nam bezpieczeństwa w trakcie popełniania przestępstwa. Musimy sobie zdawać sprawę, że nie można bezkarnie ich używać. Oczywiście wielu upiecze się i nie zostaną pociągnięci do odpowiedzialności za popełnione przy pomocy karty prepaid przestępstw. Na skuteczność jego wykrycia wpływa kilka czynników, działających zazwyczaj na korzyść przestępcy. Są to przede wszystkim waga przestępstwa, kompetencje organów ścigania bądź sądów i prokuratur, wykorzystanie nowego telefonu tylko do danego przestępstwa, współpracy operatorów komórkowych przechowujących dane telekomunikacyjne, a także z okresu retencji danych. Możemy być więc pewni, że odpowiednio szybka akcja instytucji korzystających z danych telekomunikacyjnych doprowadzi do identyfikacji odpowiedniej osoby.

Autor jest specjalistą w zakresie bilingów w aspekcie handlowym, technicznym i prawnym oraz biegłym sądowym w zakresie analizy danych generowanych przez centrale telefoniczne.

Prognozy dla rynku urządzeń mobilnych w Polsce

Damian Kowalczyk

Rok 2013 był najlepszym okresem w historii dla branży urządzeń mobilnych w Polsce. Szacuje się, że zostało sprzedanych ponad 8,5 mln sztuk tabletów i smartfonów. Już teraz widać że ten rok może być równie udany jak poprzedni.

Polacy najczęściej wybierają małoekranowe tablety i wielkoekranowe smartfony i jest to trend ogólnoświatowy. Niestety dla producentów komputerów, popularność urządzeń mobilnych wpływa na zmniejszenie zainteresowania konsumentów ich ofertą.

Eksperci przewidują że w latach 2012-2017 sprzedaż PC-tów globalnie spadnie o około 13 proc. Fenomen urządzeń mobilnych w Polsce tłumaczony jest modą na smartfony i tablety oraz faktem, iż są to relatywnie tanie urządzenia w porównaniu z innymi krajami. Polskie firmy w ostatnim czasie częściej decydowały się na wprowadzenie laptopów i smartfonów jako podstawowych narzędzi biznesowych dla swoich pracowników. Wpływ na tę sytuacje miało również przyśpieszanie jakie dokonało się w dostępie do Internetu mobilnego. Obecnie coraz więcej firm posiadających rozbudowane floty urządzeń mobilnych, dostrzega potrzebę wdrożenia rozwiązań, które będą z jednej strony lepiej zabezpieczać dane firmowe, a z drugiej zagwarantują wyższy popim bezpieczeństwa przed zagrożeniami takimi jak złośliwe oprogramowanie czy ataki hakerskie.

Według raportu firmy Ponemon Institute, która zajmuje się analizą zagrożeń na rynku urządzeń mobilnych, aż 75% osób profesjonalnie zajmujących się zabezpieczeniami IT uznało, że smarfony i tablety przysporzą im więcej pracy w 2014 roku. Ponadto 68% specjalistów od bezpieczeństwa IT odnotowało w ciągu minionych 12 miesięcy wzrost ilości ataków na urządzenia mobilne.

Jedną z kluczowych kwestii na które należy położyć większy nacisk w zakresie bezpieczeństwa firm jest edukacja pracowników. Wielu pracowników nadal nie zdaje sobie sprawy z tego, że smartfon czy tablet to urządzenia, które coraz częściej ze względu na swoje biznesowe zastosowanie staje się celem ataku dla cyberprzepców. Dlatego tak ważne jest wdrożenie zawczasu rozwiązań typu MDM, które skutecznie mogą uchronić organizacje przed tego typu zagrożeniami.

Damian Kowalczyk – specjalista w firmie Mediarecovery.