PRZESTĘPCZOŚĆ TELEINFORMATYCZNA 2015

pod redakcją
Jerzego Kosińskiego

Szczytno 2015

Recenzenci
prof. dr hab. Bernard Wiśniewski
dr hab. inż. Grzegorz Krasnodębski

Redakcja Wydawcy
Anna Bryczkowska
Piotr Cyrek
Robert Ocipiński

PUBLIKACJA ZOSTAŁA DOFINANSOWANA PRZEZ G&R S.A.

ISBN 978-83-7462-506-7
e-ISBN 978-83-7462-507-4

Druk i oprawa:
Dział Wydawnictw i Poligrafii Wyższej Szkoły Policji w Szczytnie
ul. Marszałka Józefa Piłsudskiego 111, 12-100 Szczytno
tel. 089 621 51 02, faks 089 621 54 48
e-mail: wwip@wspol.edu.pl
Objętość: 14,48 ark. wyd. (1 ark. wyd. = 40 tys. znaków typograficznych)

SPIS TREŚCI

Wstęp 5

Rozdział 1 — *Maciej KOŁODZIEJ*
Internet Rzeczy, nowe spojrzenie na ochronę prywatności 9

Rozdział 2 — *Adam E. PATKOWSKI*
Ataki ukierunkowane: „Po owocach ich poznacie je”..... 25

Rozdział 3 — *Marcin KWIECIEŃ, Paweł MORAWSKI, Krzysztof MAZUR, Tomasz KARCZEWSKI, Daniel ŻUKOWSKI*
Analiza ukierunkowanego ataku na użytkowników poczty e-mail 43

Rozdział 4 — *Krzysztof LIDERMAN*
Informacyjna ciągłość działania i ataki na sieci różnych typów..... 47

Rozdział 5 — *Neil HEPWORTH*
Wpływ zmiany podejścia do rządowej klasyfikacji bezpieczeństwa na zabezpieczenie informacji 61

Rozdział 6 — *Joanna KARCZEWSKA*
Rola audytu informatycznego w zapewnieniu bezpieczeństwa informacji..... 67

Rozdział 7 — *Jerzy CICHOWICZ*
Rekomendacje IV Forum Bezpieczeństwa Banków 75

Rozdział 8 — *Simon WISEMAN*
Wybór odpowiedniej ochrony granic sieci: zapory?, systemy nadzoru przesyłu danych?, strażnicy? 79

Rozdział 9 — *Tim FREESTONE*
Bezpieczny dostęp do poufnych informacji w środowisku pracy zespołowej 91

Rozdział 10 — *Maciej SZMIT*
Kilka uwag o ISO/IEC 27037:2012 oraz ENISA electronic evidence — a basic guide for First Responders..... 101

Rozdział 11 — *Dorota LORKIEWICZ-MUSZYŃSKA, Tomasz SIDOR*
Nie tylko biometria — możliwości identyfikacji osób z zapisów nagrań monitoringów..... 111

Rozdział 12 — *Tadeusz WIECZOREK, Magdalena ZUBAŃSKA, Krzysztof WICIAK, Marcin SZYMCZAK*
Techniczne i prawne aspekty oględzin miejsca zdarzenia z wykorzystaniem skaningu 3D 147

Rozdział 13 — *Paweł BUCHWALD, Krystian MĄCZKA, Maciej ROSTAŃSKI*
Metody pozyskiwania informacji o geolokalizacji użytkowników sieci Internet 159

Rozdział 14 — *Marcin KWIECIEŃ*
Przedstawienie translacji NAT i trudności w identyfikacji, przy braku wystarczających danych o połączeniu..... 173

Rozdział 15 — *Tomasz LADRA*
Analiza porównawcza funkcjonujących systemów służących do uzyskiwania danych stanowiących tajemnicę telekomunikacyjną..... 181

Rozdział 16 — *Paweł OLSZAR*
Złośliwe oprogramowanie w bankowości internetowej, co nowego?.... 199

Rozdział 17 — *Piotr Marek BALCERZAK*
Cyber Tarcza sektora bankowego..... 207

Rozdział 18 — *Grzegorz MATYNIAK, Jacek GARBACZEWSKI*
Dwa przypadki oszustw związanych z Allegro..... 217

Rozdział 19 — *Justyna LASKOWSKA-WITEK, Sylwester SUSZEK*
Giełda kryptowalut w redukcji ryzyka transakcji oszukańczych 229

Rozdział 20 — *Krzysztof WOJCIECHOWSKI, Artur WASZCZUK*
Odzyskiwanie haseł w komputerach przenośnych produkowanych przez IBM/Lenovo..... 235

Rozdział 21 — *Tomasz SIEMIANOWSKI*
Zarys metodologii badań przestępstw seksualnych wobec małoletnich w cyberprzestrzeni..... 245

Rozdział 22 — *Konrad KORDALEWSKI, Jerzy IWAŃSKI*
Mowa nienawiści, agresja i przemoc jako realne zagrożenie małoletniego w sieci teleinformatycznej 263

Rozdział 23 — *Damian PUCHALSKI, Michał CHORAŚ, Rafał KOZIK, Witold HOŁUBOWICZ*
Mapa drogowa CAMINO w zakresie zwalczania cyberprzestępczości i cyberterroryzmu 279

WSTĘP

W 2015 roku minęło osiemnaście lat od pierwszego seminarium nt. „Techniczne Aspekty Przestępczości Teleinformatycznej (TAPT)" zorganizowanego w Wyższej Szkole Policji w Szczytnie. Pierwsze dwie edycje seminarium gromadziły po ok. 80 uczestników, prawie wyłącznie z jednostek organizacyjnych Policji. Z czasem przybywało uczestników i w ostatnich latach, kiedy seminarium stało się międzynarodową konferencją naukowo-praktyczną, jest ich jednocześnie w Szczytnie ok. 300. Wielu z nich reprezentuje sektor prywatny, uczelnie, organizacje pozarządowe oraz inne służby i organa zajmujące się cyberprzestępczością. Tradycją jest również, że konferencja co roku ma inny temat przewodni. W 2015 roku tematem przewodnim był „*Internet of Things* i jego znaczenie w zwalczaniu i wykrywaniu cyberprzestępczości oraz ataki ukierunkowane". Internet przedmiotów może być zdefiniowany jako środowisko obiektów fizycznych, posiadających systemy wbudowane i czujniki, które łączą się z Internetem, aby dostarczyć nowych możliwości dla użytkowników końcowych. Internet przedmiotów pozwala na elastyczne świadczenie usług wszelkiego rodzaju, począwszy od automatyki domowej i usług logistycznych, po inteligentny monitoring środowiska oraz inteligentne usługi miejskie (ang. *smart city*). Miliardy ludzi korzystające już dzisiaj z Internetu i przewidywane 25 miliardów urządzeń podłączonych do Internetu do roku 2020[1] sprawiają, że Internet przedmiotów stanowi poważne wyzwanie w świecie cyfrowym, którego potencjał wpłynie na każdego człowieka i każdą działalność. Oczekuje się, że w bardzo krótkim czasie, Internet przedmiotów będzie pozwalał na wykorzystanie przez użytkownika Internetu narzędzi pomiarowych, analitycznych i wizualizacji w dowolnym czasie i dowolnym miejscu na świecie, w celu prywatnym, społecznym, na poziomie krajowym lub ogólnoświatowym. Komunikować się będą ze sobą nie tyko urządzenia. Internet przedmiotów będzie stanowił dla ludzi medium pośredniczące w komunikacji, co przyniesie kolejne problemy związane z bezpieczeństwem — wzrośnie możliwość podszywania się, kradzieży tożsamości, włamań do urządzeń i ich nieuprawnionego wykorzystania.

Obserwując dynamiczny rozwój technologii teleinformatycznych, nie sposób nie zauważyć, że Internet przedmiotów jest już elementem codziennym w kilku obszarach. Do tych obszarów zaliczyć można:

— inteligentne życie, mające na celu uczynienie życia prostszym i bezpieczniejszym dla użytkownika. Obejmuje: nowy pacjentocentryczny model opieki zdrowotnej; nowe modele sprzedaży detalicznej, w których klient jest współtwórcą podaży; konwergencję modeli bankowości; zmianę podejścia do ubezpieczeń, polegającą na odejściu od statystyk, do tworzenia polityk opartych na faktach; poprawę jakości usług publicznych, które mają być wygodne dla obywateli;

[1] Gartner: Gartner Says 4.9 Billion Connected "Things" Will Be in Use in 2015, listopad 2014, <http://www.gartner.com/newsroom/id/2905717>.

— inteligentną mobilność, mającą na celu uczynienie podróży przyjemniejszą a transport bardziej skutecznym i wiarygodnym. Inteligentna mobilność obejmuje: zarządzanie trasą w czasie rzeczywistym; autonomiczne zarządzanie jazdą samochodu; inteligentne zarządzanie ruchem (w miastach, ale także całych sieci transportowych); zarządzanie opłatami; dystrybucję i logistykę oraz zarządzanie flotą;
— inteligentne miasto, mające na celu poprawę jakości życia w miastach, obejmujących kwestie bezpieczeństwa i oszczędności energii. Inteligentne miasto obejmuje: zarządzanie infrastrukturą miasta (np. przy użyciu analiz Big Data); współpracę wielu, oddzielnych agencji przy użyciu technologii chmury; zbieranie danych za pomocą technologii mobilnych w czasie rzeczywistym, umożliwiając szybką reakcję; poprawę bezpieczeństwa publicznego i egzekwowania prawa, większą efektywność w sytuacjach kryzysowych; lepsze planowanie (np. lepsze schematy i zarządzanie projektami oraz dostawami); inteligentne liczniki i zarządzanie sieciami; zwiększoną automatyzację;
— inteligentną produkcję, mającą na celu optymalizację procesów, kontroli i jakości. Inteligentna produkcja obejmuje: uczenie maszynowe pozwalające na inteligentny, zautomatyzowany proces decyzyjny; zwiększenie interakcji i współpracy między maszynami; kontrolę i zarządzanie w sieci urządzeń produkcyjnych; optymalizowanie procesów, szybkie prototypowanie i produkcję, lepsze i bardziej wydajne procesy operacji w łańcuchu dostaw; proaktywne zarządzanie aktywami za pomocą diagnostyki i konserwacji prewencyjnych; lepszą integrację infrastruktury dzięki standardom interfejsów[2].

Tak powszechne wykorzystanie urządzeń sterowanych systemami mikroprocesorowymi, komputerów w różnej postaci, sieci teleinformatycznych musi skutkować wzrostem zagrożenia bezpieczeństwa ich użytkowników. Pojawią się nowe lub doskonalsze metody popełniania przestępstw wykorzystujące te technologie. A pamiętać należy, że przestępcy także doskonalą swoje stare, skuteczne metody[3].

Tradycyjnie, oprócz tematu przewodniego na konferencji zostały poruszone także inne pokrewne tematy, m.in.: obserwowane trendy cyberprzestępczości, bezpieczeństwo teleinformatyczne i elektronicznych instrumentów płatniczych (taże kryptowalut), bezpieczeństwo danych osobowych, monitorowanie zagrożeń w Internecie, ujawnianie, pozyskiwanie, zabezpieczanie, analiza i prezentacja dowodów cyfrowych, praktyka zwalczania cyberprzestępczości oraz narzędzia wspomagające zwalczanie cyberprzestępczości. Wszystko było rozważane w kontekście współpracy publiczno-prywatnej w zwalczaniu cyberprzestępczości.

[2] Cybersecurity and the Internet of Things, Insights on governance, risk and compliance, EY March 2015, <http://www.ey.com/Publication/vwLUAssets/EY-cybersecurity-and-the-internet-of-things/$FILE/EY-cybersecurity-and-the-internet-of-things.pdf>.

[3] Obrazują to raporty FireEye, np. Advanced Targeted Attacks: How to Protect Against the New Generation of Cyber Attacks, a także APT30 and the Mechanics of a Long-Running Cyber Espionage Operation, <http://www.fireeye.com\reports>.

Organizatorem konferencji był Instytut Badań nad Przestępczością Kryminalną i Terroryzmem, działające w nim Centrum Analityczno-Wywiadowcze i Doskonalenia Zwalczania Cyberprzestępczości przy współpracy Grupy Allegro sp. z o.o. W konferencji uczestniczyło 301 uczestników z Polski, Hiszpanii, Litwy, Rosji, Rumunii, Stanów Zjednoczonych, Wielkiej Brytanii. W czasie konferencji wygłoszono 32 referaty i przeprowadzono jedne warsztaty.

Wprowadzające w tematykę konferencji wystąpienia wygłosili prorektor ds. studenckich Wyższej Szkoły Policji w Szczytnie — insp. dr hab. Izabela Nowicka oraz kierownik ds. Współpracy z Organami Ścigania, Grupa Allegro Sp. z o.o. — Jakub Pepłoński. W pierwszym dniu konferencji wygłoszono następujące referaty:

— *Proceder wyłudzania danych osobowych i zaciągania pożyczek za pośrednictwem sieci Internet* — Jarosław Cholewiński, KWP Lublin; Kuba Kalinowski, Allegro.pl;
— *Doświadczenia w transformacji kadr Policji w zakresie zwalczania cyberprzestępczości w Wielkiej Brytanii — praktyka, wyzwania oraz przykłady dla Polski* — Aleksander Goszczycki, Matic; Sebastian Madden, PGI;
— *Wybór odpowiedniej ochrony sieci brzegowych. Zapory? Diody? Strażnicy?* — Simon Wiseman, Deep-Secure Ltd.;
— *PPP w zwalczaniu cyberprzestępczości* — Monika Wasiewicz, FBI;
— *Doświadczenia agenta FBI w zwalczaniu cyberprzestępczości* — David Crisafi, FBI;
— *Doświadczenia rumuńskie w zwalczaniu cyberprzestępczości cybercrime* — Virgiliu Pintea, Oficer łącznikowy Policji Rumuńskiej;
— *Współpraca LEA i Western Union* — Ricardas Pocius, Western Union;
— *Praktyczne ataki na aplikacje webowe* — Adam Ziaja (duży bank brytyjski);
— *Najnowsze osiągnięcia w technologii WiFi i ich możliwy wpływ na analizę kryminalistyczną* — Zbigniew Jakubowski, Compendium C.E.

W drugim dniu konferencji wygłoszono referaty na następujące tematy:

— *Ataki ukierunkowane: „Po owocach ich poznacie je”* — Adam Patkowski, WAT;
— *Trojan Slave i inne* — Jose Alemán, S21sec;
— *Przedstawienie translacji NAT i trudności w identyfikacji abonenta przy braku wystarczających danych o połączeniu* — Marcin Kwiecień, UWM Olman;
— *Jak operator wspiera walkę z cyberprzestępczością* — Przemysław Dęba, Orange;
— *Analiza ukierunkowanego ataku na użytkowników poczty e-mail* — Marcin Kwiecień, UWM Olman;
— *Weryfikacja odporności na zaawansowane, profilowane cyberataki (APT)* — Tomasz Wilczyński, EY;
— *Nie tylko biometria — możliwości identyfikacji osób z zapisów nagrań monitoringów* — Tomasz Sidor, Biuro Ekspertyz Sądowych w Lublinie; Dorota Lorkiewicz-Muszyńska, Uniwersytet Medyczny w Poznaniu;

— *Zwalczanie materiałów pornograficznych z udziałem małoletnich publikowanych w Internecie* — Martyna Różycka, Dyżurnet.pl;
— *Oszustwa z wykorzystaniem kart prepaid* — Jarosław Biegański, PayU;
— *Złośliwe oprogramowanie w bankowości internetowej — co nowego?* — Paweł Olszar, ING;
— *Doświadczenia giełdy bitcoinowej* — Sylwester Suszek, Bitbay.pl;
— *Analiza przypadków ataków skimmingowych na terenie m.st. Warszawy* — Ryszard Jurkowski, Pekao SA; Robert Jabłoński, KSP;
— *Wykorzystanie zaawansowanych technik wykrywania w badaniach dowodów cyfrowych* — Andreas Friberg, Nuix;
— *Informacyjna ciągłość działania i ataki na sieci różnych typów* — Krzysztof Liderman, WAT;
— *Rola audytu informatycznego w zapewnieniu bezpieczeństwa informacji* — Joanna Karczewska, ISACA Warszawa;
— *Monitoring — i co z tego?* — Andrzej Niemiec, PRIM;

oraz przeprowadzono warsztaty nt. Mniej szukaj, odkryj więcej za pomocą Nuix — Andreas Friberg, Nuix.

W ostatnim, trzecim, dniu konferencji wygłoszono następujące referaty:
— *Internet rzeczy a ochrona prywatności — czy dane są bezpieczne?* — Maciej Kołodziej, NK, FHU MatSoft;
— *Internetowe pole bitwy* — Bartosz Kwitkowski, Prebytes;
— *Supertimeline — wykorzystanie w technice śledczej* — Witold Sobolewski, VS Data;
— *Od 1 e-maila do kradzieży 9 milionów* — Piotr Konieczny, Niebezpiecznik.pl;
— *Praktyczna deanonimizacja użytkowników w sieci TOR* — Adam Haertle, ZaufanaTrzeciaStrona.pl;
— *Jak ścigana jest cyberprzestępczość na świecie* — Dominik Rozdziałowski, KWP Kielce;
— *Działalność centrum Badań nad Cyberprzestępczością UMK* — Arkadiusz Lach, UMK Toruń.

Zebrane w opracowaniu naukowym 23 rozdziały będące rozwinięciem i uszczegółowieniem wystąpień z konferencji TAPT, ale także poruszające nieprezentowane na konferencji tematy powinny być atrakcyjne dla wielu czytelników zainteresowanych cyberprzestępczością. Będą także przydatne dla studentów i wszystkich osób, które zajmują się zapewnieniem bezpieczeństwa, wykorzystania nowoczesnych technologii teleinformatycznych oraz ściganiem sprawców cyberprzestępstw.

Redaktorowi monografii wypada także podziękować współorganizatorowi konferencji — Grupie Allegro sp. z o.o., bez której zaangażowania całe przedsięwzięcie nie mogłoby się odbyć oraz firmie G&R S.A., która wsparła finansowo publikację monografii.

Jerzy Kosiński

Rozdział 1

INTERNET RZECZY, NOWE SPOJRZENIE NA OCHRONĘ PRYWATNOŚCI

Maciej KOŁODZIEJ[1]

STRESZCZENIE: Od kilku lat coraz większą popularność zyskuje nowy trend technologiczny zwany Internetem Rzeczy (ang. *Internet of Things IoT*[2]). Rośnie zainteresowanie IR ponieważ obejmuje on szeroki zakres tematów, także dotyczących ochrony prywatności. Z tego też powodu pojawiają się pytania jak należy korzystać z IR i jakie wymagania dotyczące ochrony danych osobowych powinny być brane pod uwagę przez jego użytkowników.
W rozdziale zebrane zostały najważniejsze, zdaniem autora, informacje opisujące pojęcie Internetu Rzeczy oraz zasygnalizowane zostały zagadnienia związane z bezpieczeństwem przetwarzania danych, z którymi mogą spotkać się użytkownicy, administratorzy oraz kontrolerzy, korzystając z infrastruktury IR i przetwarzając dane o charakterze osobowym oraz informacje o osobach, ich zachowaniu, przemieszczaniu się, cechach zdrowotnych, przyzwyczajeniach i wymaganiach.

SŁOWA KLUCZOWE: Internet Rzeczy, cyberprzestrzeń, infrastruktura, polityka ochrony danych.

Internet Rzeczy wywodzi się z koncepcji technologii Komunikacji Między Maszynowej (ang. *Machine-to-Machine*, M2M), w której wiele różnorodnych systemów i urządzeń, zbierających i przetwarzających dane, łączy się ze sobą za pomocą sieci teleinformatycznych, zazwyczaj bez udziału ludzi, świadcząc usługi i wykonując czynności na rzecz użytkowników lub ich otoczenia i środowiska.

Do świata Internetu Rzeczy nie zalicza się tradycyjnych systemów IT, gdzie końcówkami lub terminalami przetwarzającymi dane nie są zautomatyzowane urządzenia, „rzeczy", ale tradycyjne komputery z klasycznymi interfejsami (np. komputery PC, tablety, smartfony, konsole do gier itp.). W skład IR/M2M wchodzą natomiast systemy funkcjonujące samodzielnie, proste czujniki, wyposażenie domowe lub przemysłowe, skomplikowane urządzenia lub specjalistyczne oprogramowanie, które zbierają dane i wykonują operacje po ich przeanalizowaniu.

---

[1] Specjalista informatyki śledczej FHU MatSoft; konsultant ds. ochrony danych osobowych, bezpieczeństwa informacji i systemów IT; wykładowca stowarzyszony Wyższej Szkoły Policji w Szczytnie; administrator Bezpieczeństwa Informacji w Związku Pracodawców Branży Internetowej IAB Polska; wiceprezes Stowarzyszenia Administratorów Bezpieczeństwa Informacji (od 2013 r.); audytor wiodący i trener/wykładowca PECB ISO/EIC 27001; MatSoft@pro.wp.pl.

[2] Dalej jako: IR.

Jako przykłady zastosowań IR można wskazać systemy zarządzania flotą samochodów i ich monitorowanie, nadzór i sygnalizację z systemów alarmowych, automatyczne pomiary, zdalny monitoring i zarządzanie zasobami (w przemyśle, rolnictwie, gospodarce miejskiej lub środowiskowej), telemetrię, obsługę inteligentnych budynków, tagowanie towarów lub osób z użyciem znaczników RFID (ang. *Radio-Frequency IDentification*) i ich śledzenie w logistyce lub ruchu towarów i osób, zdalną robotykę i diagnostykę itp.

Internet Rzeczy rozwija się bardzo dynamicznie, mimo że nie jest to dziedzina oficjalnie wspierana i promowana. IR po prostu rośnie jako produkt kreowany przez potrzeby i nowo powstające rozwiązania, którym stawia się za cel optymalizację złożoności technologicznej i minimalizację kosztów produkcji i użytkowania, co wpisuje się w definicję Internetu Rzeczy. Coraz częściej projektowane zastosowania rozwiązań IR w gospodarstwie domowym, medycynie lub bezpośrednim otoczeniu człowieka są pilotażowo wdrażane i stają się początkiem nowych trendów w kolejnych dziedzinach. Rozwiązania takie znajdujemy na przykład w oprogramowaniu kontrolującym zawartość lodówek, odpowiedzialnym za uzupełnianie listy produktów, gdy ich braknie lub stracą ważność. IR stosowany jest też do zdalnego monitorowania stanu zdrowia pacjentów, przy kontroli zachowania ludzi na stanowiskach pracy, w trakcie uprawiania sportu lub do lokalizacji osób i mienia. Także nowoczesne odbiorniki lub dekodery telewizyjne potrafią współpracować ze środowiskiem IR wymieniając się informacjami, które z założenia mają ułatwiać dobór oferty programowej i podnosić jakoś usługi telewizyjnej. IR ma więc służyć użytkownikom, wspierać ich w podejmowaniu decyzji i kontroli otoczenia. Niestety, może też dochodzić do nadużywania dostępu do przetwarzanych informacji w celach komercyjnych lub innych nastawionych na efekt biznesowy podmiotów trzecich, niekoniecznie korzystny dla odbiorcy usługi. Czy tak jest w rzeczywistości i czy inteligentne systemy nie wpływają pośrednio na decyzje użytkowników lub czy tych decyzji nie podejmują, a informacje jakie są zbierane o użytkownikach nie są dodatkowo przetwarzane w innych celach, możliwe, że bez wiedzy osób, których dotyczą, omówione zostało w dalszej części rozdziału.

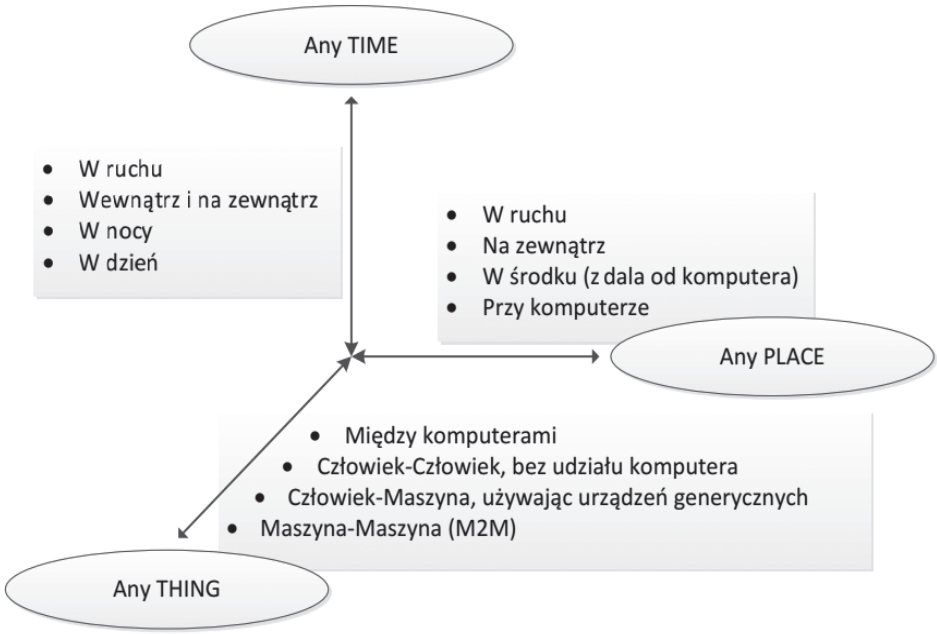
Definicje Internetu Rzeczy

Internet Rzeczy funkcjonuje w oparciu o trzy filary, odnoszące się do cech inteligentnych obiektów:

— umożliwić identyfikację siebie (wszystko jest w stanie unikalnie przedstawić się);
— zapewnić komunikację (wszystko może komunikować się);
— współdziałać (wszystko może wzajemnie na siebie oddziaływać).

Spotykana jest też alternatywna definicja Internetu Rzeczy opisująca Internet Inteligentnych Obiektów (ang. *Internet of Smart Objects*), w którym włączane do globalnej sieci urządzenia mają zdolność do samouczenia się i dzięki

temu osiągają cechy inteligencji, którą zawdzięczają możliwości komunikowania się z innymi obiektami oraz zbierania i analizowania przetwarzanych wspólnie danych, a następnie, na ich podstawie, podejmowania decyzji bazując na skomplikowanych algorytmach, dla których parametry wejściowe może ustalać operator lub generowane są na podstawie algorytmów wymiany informacji pomiędzy obiektami.



Rys. 1. Komunikacja w Internecie Rzeczy (Rekomendacja ITU-T Y.2060, 06/2012)
Źródło: A. Brachman, *Internet przedmiotów — raport*, Obserwatorium ICT, wrzesień 2013, s. 5

Coraz więcej zwolenników zyskuje, zaproponowane przez Cisco Systems, pojęcie Internetu Wszechrzeczy (ang. *Internet of Everythings*, IoE) definiowanego jako sieć łącząca ludzi, procesy, dane i przedmioty komunikujące się w sieci Internet i generujące nową wartość interoperacyjną. Rozwój technologii, w tym upowszechnienie się Internetu Przedmiotów (synonim Internetu Rzeczy), rozwiązań komunikacji mobilnej i systemów przetwarzania danych w chmurze, jak również rosnące znaczenie skomplikowanych analiz w środowiskach Big Data, pozwala na korzystanie z nowych możliwości, jakie daje koncepcja Internetu Wszechrzeczy, obejmującego całą przestrzeń przetwarzania danych w nowoczesnych systemach teleinformatycznych.

Internet Rzeczy oraz Wszechrzeczy bazują na trzech pojęciach sklasyfikowanych według ITU-T: działać zawsze, wszędzie i ze wszystkim (także z człowiekiem).

Sieci komunikacji międzymaszynowej M2M (machine-to-machine)

W chwili obecnej Internet Rzeczy zbudowany jest przede wszystkim z sieci komunikacji między urządzeniami (M2M), których podstawowe cechy to:

— heterogeniczność — czyli duże zróżnicowanie ze względu na możliwości obliczeniowe i komunikacyjne urządzeń dostarczanych przez wielu, rzadko współpracujących ze sobą producentów. Wsparcie dla heterogeniczności IR muszą zapewniać: uniwersalna architektura i stosowane zestandaryzowane protokoły;
— skalowalność — do IR będzie włączanych coraz więcej urządzeń codziennego użytku, problem skalowalności dotyczy: adresacji i nazewnictwa, wzajemnej łączności, liczby połączeń między poszczególnymi elementami sieci, ilości przesyłanych danych, zarządzania informacją i dostarczenia odpowiednich usług;
— wszechobecna wymiana danych z wykorzystaniem, najczęściej używanych, technologii bezprzewodowych, co prowadzi do ograniczeń w jakości transmisji radiowej, ze względu na prędkość i jej opóźnienia oraz do zakłóceń w transmisji i możliwości przypadkowej modyfikacji przekazywanych informacji;
— rozwiązania optymalne energetycznie, tak ze względu na koszty, jak i ekologię — zalecane jest ograniczać zużycie energii, co wiąże się ze zmniejszeniem wydajności urządzeń;
— lokalizacja i śledzenie położenia — ponieważ każde urządzenie w IR jest identyfikowane, to istnieje możliwość śledzenia jego położenia, co tworzy całkiem nowe możliwości dla logistyki kontroli. Należy jednocześnie wskazać na zagrożenie prywatności w przypadku, gdy monitoringiem objęci zostaną ludzie;
— możliwości samoorganizacji — ze względu na liczbę, ale też złożoność systemów konieczne jest zapewnienie mechanizmów samoorganizacji, samokonfiguracji, aby zminimalizować ingerencję, a także nadzór człowieka;
— zarządzanie danymi — w IR istotą jest wymiana i analiza danych. Kluczowy dla działania jest uniwersalny interfejs wymiany informacji, który jednocześnie może obniżać poziom ochrony przetwarzanych danych;
— wbudowane bezpieczeństwo i ochrona prywatności — ze względu na swoje ścisłe powiązanie ze światem rzeczywistym, technologie IR muszą zapewniać odpowiedni poziom bezpieczeństwa i prywatności.

Należy zwrócić uwagę, że realizacja bardzo rozbudowanych systemów zabezpieczeń danych może okazać się w sieciach IR trudna do uzyskania, ponieważ wiele z nich nie jest zaawansowanych technologicznie, a przez to nie ma odpowiednich zasobów pamięci lub mocy użytych procesorów, aby np. szyfrować przesyłane dane lub przechowywać je w sposób gwarantujący ochronę przed

dostępem osób lub urządzeń trzecich. Niestety, na obecnym etapie także projektanci i producenci skupiają się przede wszystkim na działaniu i komunikowaniu się urządzeń, często zostawiając zagadnienia ochrony danych do późniejszych wersji sprzętu i oprogramowania.

Komunikacja sieciowa w Internecie Rzeczy

Sieci IR wykorzystują różne technologie przewodowe i bezprzewodowe:

— sieci komunikacji komórkowej (2G, 3G i 4G {5G — LTE Dual & Multipoint Connectivity}) — urządzenia wymagają tylko doposażenia w kartę SIM i pozostawania w zasięgu danej sieci komórkowej;
— WiFi — sieci bezprzewodowe małego zasięgu, które pozwalają na podłączenie urządzeń IR do Internetu za pośrednictwem routerów lub punktów dostępowych;
— Bluetooth — protokół specjalizowany dla sieci osobistych, który umożliwia łączenie ze sobą urządzeń wyposażonych w moduł Bluetooth, dedykowany dla wymiany niewielkiej ilości danych z dużymi prędkościami transmisji;
— ZigBee — protokół dedykowany dla sieci wielopunktowych i aplikacji wymagających niskiej przepustowości, zapewnia energooszczędność urządzeniom zasilanym z baterii, przeznaczony do sieci, w której wymiana danych przebiega sporadycznie lub w której urządzenia wyposażone w czujniki bądź urządzenia wejściowe przekazują dane do ujścia (włączniki światła, liczniki, systemy bezpieczeństwa);
— Z-Wave — protokół dla domowych systemów automatyki i sterowania, szczególnie do zdalnego kontrolowania urządzeń lub oświetlenia;
— 6LoWPAN — (ang. *IPv6 over Low Power Wireless Personal Area Networks*) nazywany bezprzewodowym Internetem systemów wewnętrznych, który zapewnia lokalną obsługę protokołu IP przez niewielkie urządzenia i czujniki, tak żeby mogły być one włączone w strukturę IR.

Każdy ze sposobów komunikacji powinien być dopasowany do wymagań konkretnego elementu IR. Na łączach, gdzie występuje duża wymiana wrażliwych informacji, należy zadbać o odpowiednią jakość oraz poufność przekazu, a tam gdzie to niemożliwe należy rozważyć budowę podsystemów, z których przetworzone wstępnie informacje będą przekazywane na zewnątrz, do Internetu Rzeczy, za pomocą urządzenia pośredniczącego, agregującego i odpowiednio chroniącego dane.

Dla potrzeb komunikacji w Internecie Rzeczy przewidziano stosowanie adresacji IPv6 (protokół IP w wersji 6) lub odpowiednio skonfigurowanych systemów opartych o enkapsulację/tunelowanie transmisji w sieciach IPv4. Pojemność sieci IPv6 pozwala na tworzenie unikatowych w skali całej populacji adresów urządzeń w oparciu o niepowtarzalne numery sprzętowe MAC (IEEE 802) przyporządkowane do każdego z nich.

Przykładowo, dla adresu sprzętowego MAC 10:22:33:44:55:66 adres IPv6 w IR będzie miał postać:

64bitowy_prefiks_sieci_lokalnej:1222:33FF:FE44:5566

Adres ten powstał według następujących zasad:

— 64-bitowy prefiks sieci jest informacją rozgłaszaną przez ICMPv6 przez rutery;
— trzy najbardziej znaczące oktety identyfikatora MAC, to identyfikator producenta, w których dwa najmłodsze bity najbardziej znaczącego oktetu adresu MAC są znacznikami, które dla identyfikatorów nadanych globalnie (fabrycznie) są równe 0. Drugi z nich jest zmieniany na potrzeby IR na przeciwny;
— powiększono o 16 bitów 24-bitowy identyfikator karty, przy czym dla kart posługujących się adresem MAC brakujące bity uzupełnia się wartością FFFE.

Nadal można korzystać z automatycznego przydziału adresów IP protokołem DHCP oraz ręcznych ustawień adresacji. Gdy IPv6 nie jest obsługiwane, to połączenia IR są tunelowane do serwerów usług.

Identyfikacja „rzeczy" przepinanej lub przełączającej się między sieciami (także w związku z poruszaniem się osoby lub przedmiotu wyposażonego w tego typu czujnik lub urządzenie) będzie możliwa, ponieważ zmieniać się będzie tylko prefiks sieci lokalnej, a porównanie reszty adresu pozwoli powiązać aktywności wskazanego źródła danych. Adres taki pozwala zidentyfikować konkretne urządzenie w skali całego systemu, co daje możliwość globalnego śledzenia zakończeń IR i może prowadzić do dodatkowej analizy położenia lub zachowań obiektu, które to informacje w określonych przypadkach mogą być chronione jako dane dotyczące konkretnej osoby.

Systemy operacyjne dla Internetu Rzeczy

Ważnym zagadnieniem związanym z Internetem Rzeczy są specjalizowane systemy operacyjne dedykowane do obsługi infrastruktury i urządzeń IR. Microsoft rozwija system Windows 10 IoT Core, dla którego bezpośrednią konkurencją jest Google Brillo — system tworzony z myślą o urządzeniach IR, który zostanie zoptymalizowany dla urządzeń z bardzo ograniczoną specyfikacją sprzętową. System ten ma obsługiwać urządzenia o bardzo małej ilości pamięci RAM i z niezbyt szybkimi procesorami.

Obszary zastosowań IR

Wymienione w dalszej części rozdziału zastosowania Internetu Rzeczy to główne, ale nie jedyne kategorie aktywności i dziedziny gospodarki lub codziennego życia, które mogą być wspierane rozwiązaniami opartymi o IR. Będą się one rozwijać, a Internet Rzeczy, według niezależnych prognoz, obejmować będzie

swoim zasięgiem kolejne, stosowane obecnie rozwiązania konwencjonalne, redukując ich zasobożerność oraz złożoność operacyjną.

1. Inteligentne domy, budynki, posesje

Systemy ochrony i monitoringu (CCTV, SSWiN, SKD), utrzymania obiektów (np. ogrzewanie pomieszczeń i wody, sterowanie roletami i drzwiami, oświetlenie, systemy nawadniające) i wyposażenie AGD wyposażone w sensory, czujniki i elementy wykonawcze mogą w sposób autonomiczny nadzorować parametry użytkowe oraz środowiskowe budynków przemysłowych oraz mieszkalnych, a także terenów wokół nich, aby w zadanym, dopuszczalnym zakresie, dopasowywać parametry do wymagań lub reagować na anomalie, przekazując informacje do użytkownika obiektu lub służb nadzoru.

2. Inteligentne miasta

IR nadaje się do optymalizacji infrastruktury miejskiej (poniższy przykład opracowany jest w oparciu o wdrożone rozwiązania w Mieście Stołecznym Warszawa) poprzez zastosowanie do:

— Systemów Wspomagania Dowodzenia i Zarządzania Miastem;
— rejestracji zdarzeń i geokodowania obiektów stałych i ruchomych;
— interaktywnego pozycjonowania patroli służb miejskich;
— analizy danych i zegarów zdarzeń;
— map gęstości (natężenia) zdarzeń;
— integracji z bazami informacyjnymi:
  • PESEL — informacje zgromadzone o obywatelach,
  • CEPiK — dane o pojazdach i kierowcach,
  • „Safe-Animal" — baza właścicieli zwierząt,
— systemami pozycjonowania komunikacji miejskiej zawierającymi dane o lokalizacji taboru;
— aplikacji zawierających informacje dotyczące pojazdów, takie jak: lokalizacja, trasy dojazdów, wykonywane czynności, parametry techniczne i użytkowe.

Straż Miejska lub Policja mogą współpracować z innymi służbami i podmiotami korzystając z danych udostępnianych przez ich systemy IR i dzieląc się posiadanymi informacjami.

Przykładem może być aplikacja „GeoAlert" udostępniona przez stołeczne zakłady komunikacyjne, za pomocą której można ustalić lokalizację poruszającego się taboru, a uruchomiona usługa „SMS interwencyjny" umożliwia pasażerom zgłoszenie zdarzeń niebezpiecznych w konkretnym pojeździe. Bezpośredni przekaz informacji sprawia, że szybciej i skuteczniej można podjąć interwencję, jednocześnie dokumentując jej przebieg i zadbać o bezpieczeństwo pasażerów i motorniczych.

Drugim przykładem może być współpraca z jedną z komend rejonowych Policji w Warszawie. Na podstawie udostępnionych przez nią danych stworzono mapy kradzieży samochodów na terenie dzielnicy (mapę punktową, następnie

czasową i gęstościową). Na ich podstawie zdecydowano o dyslokacji patroli (biorąc pod uwagę konkretne regiony, w których występowało natężenie zdarzeń, a także okresy czasowe, które można było odczytać na podstawie zegarów obrazujących natężenie zjawiska z podziałem na godziny i dni tygodnia). Wyniki analiz zostały przekazane do koordynacji w komendzie stołecznej Policji. Wyniki akcji były pozytywne, doszło do zatrzymania złodziei samochodów

W dużych miastach uruchamiane są systemy automatycznej obserwacji oraz identyfikacji osób i pojazdów poruszających się w ciągach komunikacyjnych. Pozwala to na stały nadzór i sprawne odszukanie a następnie śledzenie konkretnych pojazdów lub np. podejrzanych osób. Często odbywa się to bez wiedzy zainteresowanych, którzy nie są poinformowani, ani o celach, ani o zakresie i możliwościach operacyjnych takich systemów.

3. Monitoring pojazdów

Kolejnym obszarem, w który wkraczają rozwiązania IR jest monitoring pojazdów wykorzystujący systemy GPS oraz infrastrukturę nadzoru znajdującą się wzdłuż dróg.

Poniżej podane zostały przykładowe informacje, które np. pracodawca może uzyskać z systemu:

— informacja o obecnej lokalizacji pojazdu i przebytej trasie;
— informacja o prędkości i ilości obrotów silnika;
— przyspieszenie w trzech osiach;
— używany obecnie bieg;
— informacja o paliwie;
— informacja o ciśnieniu opon;
— informacja o awarii pojazdu;
— informacje o dynamice jazdy, gwałtownym przyspieszaniu, hamowaniu;
— kto prowadzi pojazd (w tym zdjęcie kierowcy);
— transmisja audio/wideo z kabiny lub otoczenia pojazdu.

Część systemów wyposażonych jest też w mechanizmy pozwalające na zdalne wpływanie na działanie pojazdu i komunikację dwukierunkową z kabiną.

Wszystkie przetwarzane parametry służą nadzorowi bezpieczeństwa ruchu oraz stanu pojazdu, ale niewłaściwie wykorzystane lub zestawiane mogą stanowić również zestaw danych opisujących szczegółowo kierowcę i jego zachowanie w pojeździe, a to można uznać za informacje opisujące cechy osobowe monitorowanego kierowcy, które powinny być dołączone do rekordu zawierającego jego dane osobowe i chronione w sposób, który definiują przepisy szczególne, a który może nie być dostępny w środowisku Internetu Rzeczy.

4. Inteligentne sieci medyczne

Ludzie starsi potrzebują więcej opieki, a to napędza przemysł i usługodawców w kierunku rozwoju mikroprocedur medycznych, telemedycyny i porad paramedycznych.

Już w chwili obecnej można monitorować i przekazywać informacje do osób nadzorujących stan pacjenta, śledzić wybrane parametry diagnostyczne i sygnały fizjologiczne, np. temperaturę, ciśnienie krwi, czynności oddechowe. Nie stanowi też problemu zbieranie danych dotyczących aktywności podopiecznych, możliwa jest kontrola wykonania procedur medycznych oraz zdalna analiza nawyków żywieniowych. Coraz powszechniejsza jest też zdalna kontrola i zarządzanie osobistymi urządzeniami medycznymi (np. rozrusznikami serca, urządzeniami EKG, rejestratorami Holter, pompami insulinowymi itp.). Dostępne są rozwiązania przemysłowe, które monitorują pozycję pracownika i w przypadku, gdy zbyt długo przebywa w niestandardowym ułożeniu ciała (np. długo siedzi lub leży) czujniki przekazują sygnał alarmowy do systemu powiadamiania.

5. Inteligentne przedsiębiorstwa i przemysł

Technologie radiowych identyfikatorów (RFID) znajdują powszechnie zastosowanie w wielu przedsiębiorstwach w procesach sterowania łańcuchem dostaw. Każdy towar, półprodukt lub składnik dający się „otagować/oczipować" posiada swój chip RFID i dzięki temu w sposób automatyczny można zidentyfikować, gdzie i ile materiałów się znajduje. Wykorzystanie tych rozwiązań jest podstawą funkcjonowania sprawnej logistyki, a bieżący nadzór nad towarami i półproduktami znajdującymi się na każdym etapie produkcji (także magazynowania, dostaw półproduktów i wysyłki gotowego towaru) jest koniecznością.

Technologia może być wykorzystana także do dostarczenia konsumentowi lub użytkownikowi informacji na temat zakupionego produktu. Odpowiednio przygotowany chip RFID może udostępnić np. informacje o sposobie obsługi lub użytkowania, dacie ważności, aktualnym stanie jakościowym, zaleceniach producenta i wielu innych.

Identyfikacja obiektów ma również zastosowanie w systemach zapobiegania kradzieżom (dzięki stosowaniu systemów bramek kontrolnych i nadzorowi nad ruchem towarów) oraz w walce z podróbkami (w oryginalnych produktach lub w ich opakowaniach zbiorczych umieszczone mogą być identyfikatory RFID informujące o unikalnych cechach identyfikacyjnych produktu).

RFID znajduje zastosowanie w kompleksowym monitoringu ruchu pracowników, a współpracując z systemem wideo monitoring pozwala na identyfikację konkretnych osób, których dane są przetwarzane w kontrolerach odpowiedzialnych za działanie infrastruktury.

6. Inteligentne systemy energetyczne i pomiarowe

Współczesne sieci energetyczne działają najczęściej w oparciu o prognozę zużycia energii powstającą na bazie danych historycznych. Prognozy te stanowią jedynie przybliżenie rzeczywistego zużycia i nie pozwalają reagować, na przykład na okresowe zmiany zapotrzebowania mocy, chwilowe przeciążenia czy nadwyżki mocy ze źródeł alternatywnych.

Rewolucja w systemach pomiarowych i wprowadzenie rozwiązań Internetu Rzeczy rozpoczęła się od zdalnego odczytywania danych z liczników, kontroli statusów, reagowania na alarmy, czyli wprowadzenia do powszechnego użytku automatycznych systemów pomiarowych (ang. *Automatic Meter Reading*). Rozbudowanie inteligencji w systemach pomiarowych (ang. *Smart Metering*) jest konieczne dla współdziałania z inteligentnymi systemami energetycznymi, które już dziś potrafią automatycznie zarządzać bilansem mocy i jej sprzedażą w przypadku nadwyżek.

Zautomatyzowanie procesów po stronie odbiorcy, natychmiastowe rozliczenia i rachunki za faktycznie zużyte dobra (energia elektryczna, gaz, woda, ciepło), możliwości zdalnej zmiany taryfy dostosowującej model płatności do parametrów zużycia, blokowanie instalacji w przypadku nadużyć lub zaległości płatniczych, zbieranie danych statystycznych dotyczących dostarczonej i pobranej energii, bieżący monitoring itp. możliwe są obecnie zdalnie, z wykorzystaniem nowoczesnych liczników energii.

7. Systemy monitorowania środowiska

Kluczową rolę dla monitoringu środowiska odgrywa rozległa sieć czujników o małym poborze mocy, które zbierają dane dotyczące temperatury, wiatru, opadów deszczu, wysokość poziomu rzek itp. oraz przekazywanie ich w łatwy i niskobudżetowy sposób do centrów monitoringu.

Duże systemy hydrotechniczne objęte są obecnie nadzorem i zarządzane w oparciu o systemy o cechach zbliżonych do specyfikacji M2M. Można więc zakwalifikować je jako składniki Internetu Rzeczy, mimo że w ich projektach nie umieszczono takich powiązań.

Stosowanie czujników i urządzeń wykonawczych w systemach przeciwpożarowych w lasach lub dużych skupiskach miejskich, które po wykryciu ognia, same skontaktują się ze strażą pożarną, co znacząco skróci czas reakcji na zaistniałe zdarzenia, wskazuje na aktualne trendy w tej dziedzinie. Często systemy te, korzystając z czujników innego typu, będą w stanie udostępnić służbom ratunkowym bieżące informacje o obecności ludzi w miejscu wystąpienia zagrożenia pożarowego, a także o rodzaju palnych materiałów czy stopniu zajęcia obszaru ogniem.

Przykłady zastosowań Internetu Rzeczy

O tym, jak duże jest spektrum potencjalnych zastosowań dla Internetu Rzeczy, świadczyć mogą zrealizowanie z pozytywnym skutkiem projekty oraz zestawienie branż, w których już obecnie działają systemy dające się zakwalifikować jako składniki Internetu Rzeczy.

Część rozwiązań wprawdzie oceniane jest jako nieciekawa i mało przydatna do użytkowania w dużej skali, ale znajdują one odbiorców i naśladowców, często pasjonatów, którzy rozwijają możliwości i poprawiają parametry funkcjonalne.

Poniżej przedstawiono kilka przykładowych, dostępnych rozwiązań spełniających kryteria IR:

— inteligentny budzik, który zadzwoni wcześniej, jeśli ruch w okolicy (informacje pozyskane z czujników na skrzyżowaniach) lub korki na zazwyczaj wybieranej drodze do pracy (komunikacja z urządzeniami kontroli ruchu w pojazdach i infrastrukturze drogowej) są większe;
— rośliny (a dokładnie — czujniki zainstalowane w donicach) automatycznie informują system ogrodniczy, kiedy należy je podlać lub uruchomić nawożenie;
— buty do biegania (wyposażone w sensory ruchu) nadzorując: czas, prędkość i przebyty dystans, dają możliwość oceny postępów (wizualizacja ma miejsce na zegarku z systemem joggingowym), ale możliwa jest także rywalizacja z innym biegaczem znajdującym się w dowolnym miejscu na Ziemi (wykorzystując platformy informacyjne w klubach i stowarzyszeniach sportowych);
— inteligentny pojemnik na lekarstwa może sygnalizować pacjentowi, ale również poinformować nadzorujący go personel medyczny, że nie przyjęto leku (sprawdzenie otwarcia pojemnika lub wydania dawki). W przypadku potwierdzenia przyjęcia leku (pochodzącego z odpowiedniego czujnika IR) można dodatkowo skontrolować, czy inne sensory znajdujące się w otoczeniu pacjenta potwierdzają wykonanie czynności mających na celu zażycie lekarstwa (np. czy z lodówki wyciągnięto butelkę z wodą do popicia leku, użyto pompy insulinowej lub czy pacjent udał się odpoczynek po zastrzyku itp.);
— monitoring wolnych miejsc parkingowych (czujniki zajętości obszaru, dość powszechnie stosowane na dużych parkingach) może wpłynąć na mechanizmy kierowania strumieni turystów lub klientów (dzięki współpracy z inteligentną sygnalizacją świetlną) w celu rozładowania korków na parkingach, ale również na drogach dojazdowych;
— inteligentne węzły kontrolne na bramownicach umożliwiają sterowanie sygnalizacją świetlną na skrzyżowaniach i sterowanie ruchem w dużych ciągach komunikacyjnych (wykorzystując dodatkowo pętle indukcyjne lub strefowanie obrazu) eliminując chwilowe korki i wpływając na długoterminowe zmiany charakterystyki ruchu. Urządzenia te dają też możliwość obserwacji pojazdów (kamery CCTV) oraz wykrywanie wykroczeń drogowych (także przez odcinkowy pomiar prędkości i kontrolę stosowania się do sygnalizacji świetlnej);
— w pojazdach komunikacji zbiorowej powszechnie stosowany jest obecnie zdalny nadzór wideo (z wykorzystaniem kamer współpracujących z urządzeniami GSM) i sygnalizacja problemów oraz zagrożeń (dzięki przyciskom bezpieczeństwa), dzięki czemu dyspozytorzy oraz służby porządkowe mają możliwość sprawnie reagować na docierające z pojazdów informacje;

— w fazie testów są autonomiczne pojazdy (wyposażone w czujniki parametrów ruchu, antykolizyjne, logistyczne) dowożące towary zamówione przez systemy magazynowe (wyposażone w czujniki na półkach lub spięte z systemem logistycznym);
— dzięki integracji IR z firmami kurierskimi możliwe jest dostarczenie produktów do domowej lodówki, jeśli tylko czujniki w lodówce stwierdzą braki i złożą odpowiednie zamówienie.

Przepisy, bezpieczeństwo oraz bariery prawne dla Internetu Rzeczy

Zachowanie poufności i prywatności w Internecie Rzeczy jest bardzo ważnym zagadnieniem dla osób prywatnych, firm i organizacji. Rozwiązania technologiczne, gwarantujące bezpieczeństwo to zbyt mało, aby zapewnić wystarczającą ochronę wszystkim użytkownikom.

Istniejące regulacje i przepisy prawne muszą być dostosowane do nowej rzeczywistości, którą przynoszą Internet Rzeczy oraz Internet Wszechrzeczy. Wiele krajów nie nadąża z tworzeniem nowoczesnych norm prawnych. Z tego powodu proces tworzenia prawa uległ decentralizacji, przenosząc nacisk na procesy deregulacyjne oraz samoregulację. Tworzenie norm funkcjonowania w sieci przekazano organizacjom społecznym i gospodarczym, które często w drodze samoregulacji i dobrych praktyk branżowych tworzą zasady dostosowane do wymogów stawianych technologiom dostępnym w Internecie Rzeczy.

Problemem jest też zasięg nowych przepisów. Wydaje się, że stworzenie wyłącznie prawa krajowego, w każdym kraju wedle lokalnych zasad, nie będzie wystarczające. Brak granic dla technologii musiałby iść w parze z tworzeniem uniwersalnego, ponadgranicznego prawa i przepisów o zasięgu ogólnoświatowym, a przynajmniej europejskim, podobnie jak to jest czynione w przypadku prawa ochrony danych i ogólnie prawa do prywatności w Unii Europejskiej.

Rozszerzanie zasięgu przepisów i regulacji dotyczą nie tylko kwestii bezpieczeństwa. Problem ten dotyczy, m.in. regulacji w zakresie wykorzystania pasma radiowego oraz norm związanych z promieniowaniem elektromagnetycznym, ochroną środowiska i energetyką.

Bezpieczeństwo informacji w Internecie Rzeczy

Wiele danych gromadzonych w systemach IR może mieć charakter wrażliwy, opisując informacje osobowe, aktywności i zachowania osób, przedsiębiorstw i urządzeń. Problem bezpieczeństwa danych i procesów w IR należy rozpatrywać nie tylko pod kątem ochrony treści informacji, ale też z uwzględnieniem jej innych cech, takich jak autentyczność, nienaruszalność czy aktualność. Zakłócenie

w jednym z ogniw systemu opartego o IR może spowodować zaburzenia w pracy innych, współpracujących ze sobą elementów, a efekt domina spowoduje, że zakłócenia występujące w jednym miejscu sieci będą automatycznie propagowane do innych węzłów.

Przewiduje się, że w ciągu 10 lat w sieci znajdzie się około 50 miliardów urządzeń, dla których konieczne będzie wprowadzenie ścisłych procedur ochrony terminali i sensorów końcowych.

Ciągła komunikacja pomiędzy urządzeniami podnosi prawdopodobieństwo wielokrotnego przetwarzania, przesyłania, a przez to narażania informacji na zagrożenia. Podniesienie bezpieczeństwa często, niestety, oznacza ograniczenie dostępności.

Wraz z rozwojem technologii zwiększa się też pole do nadużyć, co przy słabym obecnie wsparciu dla mechanizmów ochrony rozwiązań Internetu Rzeczy stanowić może zagrożenie dla osoby, która jest monitorowana. Czujniki mogą działać na jej korzyść, ale jeśli np. ktoś nieuprawniony uzyska zdalny dostęp do sterownika rozrusznika serca lub wpłynie na parametry modułu zarządzania pojazdem zatrzymując go w sposób niezależny od kierowcy (a nie jest to niestety fantastyka naukowa) może spowodować zagrożenie dla zdrowia lub życia. Także dostęp do informacji i prowadzenie analiz przez osoby nieuprawnione lub np. możliwość pozyskania informacji z systemów monitorowania obiektów o obecności w nich osób lub mienia, albo zdalne monitorowanie pracowników ile czasu spędzają poza stanowiskiem pracy, mogą być wykorzystane przez innych w sposób niezgodny z pierwotnym celem ich przetwarzania, także ze szkodą dla użytkowników/właścicieli danych.

Inteligentne systemy pomiarowe dodają do katalogu zagrożenia dla prywatności odbiorców. Wbudowane w liczniki narzędzia diagnostyczno-pomiarowe pozwalają dość dokładnie określić parametry włączanego odbiornika energii, a od identyfikacji konkretnego urządzenia i parametrów jego pracy na przestrzeni doby, tygodnia lub miesiąca do powiązania go z użytkownikiem ścieżka jest krótka, a pojawiają się duże możliwości zbierania danych o zachowaniu się odbiorcy i naruszenia jego prywatności lub nawet bezpieczeństwa.

Dla każdej kategorii rozwiązań należy przeprowadzić odpowiednią analizę zagrożeń dla prywatności i wdrożyć mechanizmy pozwalające kontrolować przepływ informacji dotyczących konkretnych osób lub ich zachowań.

Technologia w najważniejszych obszarach IR

Technologia Internetu rzeczy podlega ciągłym zmianom i rozwojowi. Planuje się, że do 2020 roku wprowadzone zostaną już rozwiązania, które w sposób kompleksowy zapewnią, oprócz złożonej i wszechstronnej funkcjonalności urządzeń, także adekwatną do potrzeb ochronę danych w nich przetwarzanych. Tabela 1 wskazuje trendy i obszary zmian przewidzianych do wdrożenia w IR.

Tabela 1. Trendy i obszary zmian przewidzianych do wdrożenia w IR

	2012-2015	2015-2020	2020 i później
Technologie identyfikacji	Ujednolicone środowisko identyfikacji obiektów Otwarty interfejs dla sieci Internetu rzeczy	Zarządzanie identyfikacją Technologie semantyczne Zapewnienie prywatności	Identyfikacja za pomocą „kodu DNA rzeczy”
Architektura	Zdefiniowanie architektury Internetu rzeczy Sieć dla sieci architektur Zasady współdziałania między platformami	Architektura adaptacyjna bazująca na kontekście Mechanizmy samo* (samo-organizacji, konfiguracji, optymalizacji, rekonfiguracji, ochrony, lokalizacji, zasilania)	Architektury kognitywne Architektury empiryczne
Sieć	Sieci samoświadome treści Sieci samoorganizujące się Transparentna lokalizacja sensorów Sieci niewrażliwe na opóźnienia Sieci przechowywania danych Hybrydowe technologie sieciowe	Dalszy rozwój sieci świadomych treści	Sieci kognitywne Sieci samouczące się Sieci samo naprawiające się
Aplikacje	Rozwój technologii semantycznych Aplikacje sieci społecznych	Aplikacje zorientowane na cel Rozproszona inteligencja Środowiska M2M	Aplikacje zorientowane na użytkownika Aplikacje Człowiek-Maszyna
Bezpieczeństwo	Zorientowane na użytkownika zapewnianie prywatności oparte na treści i wymaganiach Przetwarzanie danych z uwzględnieniem prywatności danych Wirtualizacja i anonimizacja	Profile bezpieczeństwa i gwarancji prywatności oparte na potrzebach Bezpieczeństwo oparte na treści	Samo adaptacja stosowanych zasad bezpieczeństwa i bezpieczeństwa protokołów

The Internet of things, 2012 New Horizons, European Research Cluster on the Internet of things. Dr. Ovidiu Vermesan et al. Internet of Things Strategic Research Roadmap

Podsumowanie

Internet Rzeczy nie daje obecnie odpowiedzi, jak można w sposób bezpieczny skorzystać z przetwarzanych informacji. Mimo pierwszych wzmianek o IR datowanych na przełom wieku XX i XXI nadal wiele tematów pozostaje do zdefiniowania, opracowania i zrozumienia, tak przez projektantów, jak i użytkowników Internetu Rzeczy.

Celem rozdziału było usystematyzowanie wiedzy o Internecie Rzeczy i sygnalizacja, że jest to obszar, który w kolejnych latach będzie wymagał więcej uwagi pod względem procedur bezpieczeństwa, ale także procedur ochrony, dochodzeniowo-śledczych oraz optymalizacji wykorzystania tam, gdzie IR powinien zostać zastosowany.

Nie było zamierzeniem autora wskazywanie sposobów prowadzenia działań rozpoznawczych i dochodzeniowych w przestrzeni Internetu Rzeczy, chociaż wiele z nich można wskazać wśród przedstawionych realizacji praktycznych IR. Każda technologia i rozwiązanie mogą być wykorzystywane na wiele sposobów, dlatego na potrzeby poszukiwania odpowiedzi na pytanie „Kto jest sprawcą?" Internet Rzeczy udostępnia wiele narzędzi, z pomocą których można przeanalizować wiele z wymienionych obszarów aktywności rzeczy w IR i na ich podstawie wyciągać wnioski dowodowe. Internet Rzeczy udostępnia informacje m.in. z: systemów sterowania i nadzoru nad ruchem ulicznym, zarządzania inteligentnym domem i jego otoczeniem, systemów alarmowych SSWiN, monitoringu wideo CCTV, inteligentnych liczników energii, monitorowania zużycia zasobów i warunków środowiskowych, aplikacji i urządzeń służących do nadzoru nad stanem zdrowia, geolokalizacji telefonów lub aktywności osób i ich urządzeń w Internecie, wykorzystania infrastruktury usługowej i identyfikacji jej użytkowników, podglądu ekranów telewizorów, urządzeń multimedialnych SetTopBox i konsol rozrywki domowej, systemów inwentaryzacji i list zakupów w lodówkach itp.

Rozdział ten nie jest też miejscem dla omawiania szczegółowych przepisów na wykonanie „przeszukań na odległość" z wykorzystaniem IR, mimo że to, między innymi, Internet Rzeczy może ułatwiać ich realizację, ponieważ np.:

— sprawdzenie, kto konkretnie lub ile osób przebywa aktualnie lub było w lokalu;
— kontrola zawartości lodówki lub co i kiedy praliśmy w pralce;
— ustalenie zainteresowań na podstawie rejestru oglądanych programów telewizyjnych;
— analiza ostatnich lub aktualnych podróży samochodem;
— sprawdzenie historii zmian konkretnych parametrów rejestrowanych przez dowolnego typu czujniki włączone do IR;

jest możliwe i zadania te nie stanowią już futurystycznych wyzwań.

Dlatego też prawnicy mają obecnie wiele wątpliwości, jak dopuścić do procesu dowody zabrane z użyciem technologii, która nie jest przewidziana w przepisach.

Mimo że w chwili obecnej rozwiązania Internetu Rzeczy nie są jeszcze popularne, a projekty dotyczące IR są bardziej wyspami tematycznymi niż kompletnymi i spójnymi systemami przetwarzania informacji, to obserwując trendy rynkowe można uznać, że coraz więcej rozwiązań budowanych będzie w oparciu o niewielkie, specjalizowane urządzenia, których współpraca pozwoli na pełne odwzorowanie parametrów środowiskowych, zdarzeń, faktów i ich zmian w systemach przetwarzających informację. Dlatego konieczne będzie odmienne spojrzenie na ochronę prywatności, a szczególnie na zbiory danych osobowych i zbierane w nich informacje, ponieważ dane mogą być podzielone pomiędzy wiele urządzeń, a ich przetwarzanie będzie wnosiło nowe, dotychczas nieuwzględniane typy i kategorie danych o osobach i ich zachowaniu lub unikalnych cechach.

Problemem może być także dokładne określenie miejsca przetwarzania danych, ponieważ powszechność stosowanych w Internecie Rzeczy rozwiązań chmurowych (ang. *Cloud Computing*), usprawniających proces obróbki informacji, może doprowadzić do sytuacji, w której operatorzy, a nawet administratorzy danych nie będą znali lokalizacji, ani treści danych pośrednich, nie mając dostępu do danych źródłowych z końcówek, czujników i sensorów IR, a w zamian uzyskując dane lub decyzje końcowe, powstające jako wynik pracy złożonego systemu.

Nowego znaczenia nabrać może też proces anonimizacji, czy usuwania informacji, w którym dane powinny być, tam gdzie to możliwe i uzasadnione, pozbawiane cech pozwalających na identyfikację osób, których dotyczą. Należy więc ostrożnie podchodzić do Internetu Rzeczy i w sposób świadomy korzystać z możliwości przetwarzania w nim danych osobowych.

Bibliografia

1. Brachman A., *Internet przedmiotów — raport*, Obserwatorium ICT, wrzesień 2013.
2. Gajewski M., *Czym jest Internet Wszechrzeczy?*, „Chip", czerwiec 2013.
3. *Internet przedmiotów — nowa rzeczywistość czy science fiction ?*, „WP Tech", maj 2013.
4. Kołodziej M., *Internet rzeczy a ochrona prywatności — czy dane są i będą bezpieczne?*, „Ochrona Danych Osobowych WiP" 2015, nr 11, sierpień 2015.
5. Materiały konferencyjne: „Internet Rzeczy. Bezpieczeństwo Smart City", VII Konferencja Naukowa Bezpieczeństwo w Internecie, UKSW, maj 2015.
6. Wiewiórowski W., *Problem kontroli nad informacjami będzie narastał*, „Gazeta Prawna", grudzień 2014.
7. Wrzos W., *Internet rzeczy: Będziemy celem ataków*, „Komputer Świat", lipiec 2014.

Rozdział 2

ATAKI UKIERUNKOWANE: „PO OWOCACH ICH POZNACIE JE”[1]

dr inż. Adam E. PATKOWSKI[2]

STRESZCZENIE: W rozdziale przedstawiono problem obrony przed zdalnymi atakami, które są słabo wykrywalne poza warstwą aplikacji. Zaprezentowano wybrane rodzaje ataków kombinowanych i specyfikę ataków ukierunkowanych. Wskazano rozwiązanie pozwalające na rozpoznawanie symptomów ataków (lub powodzenia ataków) i włączenia go w klasyczne systemy zabezpieczeń sieciowych. Proponowane rozwiązanie przeznaczone jest do wbudowania w nowo projektowane aplikacje.

SŁOWA KLUCZOWE: cyberatak, atak ukierunkowany, ochrona, IDS, behawior, system zabezpieczeń.

1. Geneza

W Wojskowej Akademii Technicznej prowadzone są m.in. prace związane z problemami ochrony przed „cyberatakami” systemów teleinformatycznych zaliczanych do infrastruktury krytycznej. Przez „cybertak” rozumie się w tym szczególnym przypadku wszelkie oddziaływania z wykorzystaniem środków informatycznych, w szczególności oddziaływania, w których medium transmisyjnym na dowolnym etapie jest ruch sieciowy. W niniejszym opracowaniu dalej mowa jest o atakach złożonych, w których napastnik lub napastnicy, a także ludzie bądź narzędzia działające na ich rzecz, wykonują działania wykraczające poza wykorzystanie środków lub sposobów leżących w dziedzinie teleinformatyki. Nie zmienia to jednak faktu, że generalny proces ataku w ostatecznym rachunku wypełnia definicję ataku informacyjnego, czyli jest:

— oddziaływaniem na szkodę interesów pewnego podmiotu;
— działaniem celowym;
— skierowany przeciw zasobom informacyjnym (chociaż być może niepozostającym w administracji podmiotu);
— zmierzał do obniżenia („pogorszenia”) wartości miar atrybutów bezpieczeństwa informacji tych zasobów informacyjnych.

---

[1] Mt. 7: 16: *Poznacie ich po ich owocach. Czy zbiera się winogrona z cierni lub figi z ostów* — bp K. Romaniuk (opr.), *Ewangelia wg św. Mateusza*. Biblioteka „Niedzieli”, Częstochowa 2007.

[2] Instytut Automatyki i Robotyki, Wojskowa Akademia Techniczna, <aep@ita.wat.edu.pl>.

Ataki informacyjne to celowe próby obniżenia miar atrybutów bezpieczeństwa informacji: tajności, integralności lub dostępności wykonywane na szkodę interesów ofiary. Nie oznacza to, że wszystkie szczególne techniki działania użyte do osiągnięcia takich generalnych celów złożonych ataków informacyjnych muszą leżeć w dziedzinach *stricte* teleinformatycznych, a nawet technicznych.

Podczas wspomnianych przedsięwzięć związanych z obroną pewnych systemów teleinformatycznych infrastruktury krytycznej prowadzone są m.in. badania techniczne bezpieczeństwa. Szczególnie frustrujące dla wykonawców jest badanie z wykorzystaniem tzw. czarnych scenariuszy, gdzie zakłada się, że napastnik wie wszystko o celu ataku, ma do dyspozycji wszelkie możliwe środki, w tym nowe, nieznane obrońcom exploity[3], ponadto ma po swej stronie statystykę, a zapewne i prawo Murhy'ego… Co gorsza, należy założyć, że napastnik zna zarówno owe słabości, jak i exploity, bo jest to jedyny sposób zasymulowania przyszłych, wysoce prawdopodobnych, jak uczy doświadczenie, sytuacji. Określenie „mieć przeciw sobie statystykę" to odniesienie do częstych w praktyce obrońców sytuacji, gdy muszą zabezpieczyć wszystkie potencjalne słabości, gdy napastnikowi do sukcesu wystarczy tylko jedna pominięta. To podejście jest bliskie sytuacji, która występuje podczas tzw. ataków ukierunkowanych (ang. *targeted attack*). W pewnym uproszczeniu ataki ukierunkowane to wymierzone w zasoby informacyjne ataki, prowadzone za pomocą technik i narzędzi przygotowanych lub modyfikowanych specjalnie na potrzeby każdego z ataków[4].

2. Repertuar napastnika

Zwykle w doniesieniach medialnych najwięcej miejsca zajmują doniesienia o nowo odkrytych słabościach oprogramowania, co powoduje, że inne dziedziny są zapominane. CAPEC (ang. *Common Attack Enumeration and Classification*[5]) definiuje sześć[6] głównych dziedzin ataków (por. rys. 1, lewa kolumna), określając zbiory ich celów:

— Ludzie (*social engineering*);
— Łańcuchy dostaw;
— Komunikacja;
— **Oprogramowanie;**

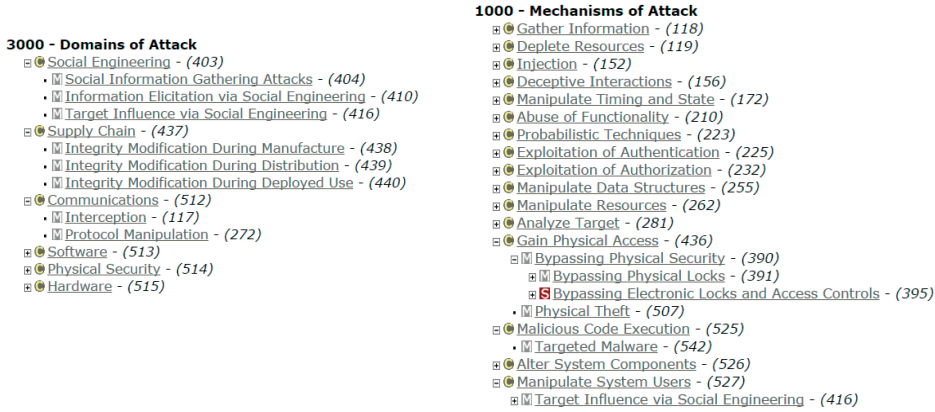
[3] Przez exploit rozumie się tu „rutynowy algorytm (często w postaci skryptu lub programu) wykorzystania słabości systemu na szkodę jego bezpieczeństwa".

[4] Por. *Targeted cyber attacks*. GFI White Paper. GFI 2009, <http://www.gfi.com/whitepapers/cyber-attacks.pdf>.

[5] *Common Attack Pattern Enumeration and Classification. CAPEC List Version 2.6.* The MITRE Corporation, http://capec.mitre.org, Status: last updated: December 04, 2014.

[6] <http://capec.mitre.org/data/definitions/3000.html>.

— Bezpieczeństwo fizyczne;
— Sprzęt;
rozwijanych (do czterech poziomów w głąb) na bardziej szczegółowe poddziedziny.



Rys. 1. CAPEC — definicje głównych domen i klas technik ataków
Źródło: Common Attack Pattern Enumeration…, wyd. cyt.

Definicje klasyfikacyjne technik ataków[7] według CAPEC (por. rys. 1, prawa kolumna) również ułożono w postaci drzewiastej struktury. Najwyższy poziom to kategorie ataków (poniżej i na rysunku niektóre z kategorii, dla ilustracji, rozwinięto na zbiory technik niższego poziomu klasyfikacyjnego):
— Zbieranie informacji.
— Wyczerpywanie zasobów.
— Wstrzykiwanie.
— Działania oszukańcze.
— Manipulacje czasem lub stanem.
— Zakłócenia działania.
— Techniki probabilistyczne.
— Wykorzystywanie uwierzytelniania.
— Wykorzystywanie autoryzacji.
— Manipulowanie strukturami danych.
— Manipulowanie zasobami.
— Zdobywanie dostępu fizycznego:
  • Przenikanie ochrony fizycznej,
  • Kradzież sprzętu lub nośników informacji.
— Wykonywanie niepożądanego kodu.
— Podmiana elementów systemu.

[7] <http://capec.mitre.org/data/definitions/1000.html>.

— Manipulowanie użytkownikami:
  • Wpływ na cel za pomocą *social engineering*.

Napastnicy mogą swobodnie wykorzystywać środki z różnych dziedzin i kategorii.

3. Niedostrzegane zagrożenia

W CAPEC nie wymieniono jawnie pewnej klasy zagrożeń związanych z obdarzaniem zaufaniem dostawców oprogramowania. Każdy praktycznie komputer zawiera oprogramowanie, którego producenci oraz pośrednicy w dostarczaniu („łańcuch dostaw") są nieomal poza podejrzeniem — komputer jest kupowany z domniemaniem, że jest wolny od wrogiego kodu i niepożądanych funkcji. Co ciekawe, późniejsze aktualizacje oprogramowania nie są już traktowane z tak bezkrytyczną ufnością, ale obniżenie zaufania dotyczy elementów łańcucha dostaw, a nie wydawców poprawek. Producenci pozostają nadal poza podejrzeniem.

Z rzadka pojawiają się głosy, że np. Microsoft lub dowolna z wielkich firm antywirusowych[8] mogłyby wyłączyć lub sparaliżować dowolny podzbiór komputerów. Np. określony według wersji językowej oprogramowania. W ogólności wydaje się to obiecującym środkiem oddziaływania na gospodarkę przeciwnika w początkowej fazie konfliktu zbrojnego. Co więcej — mechanizmy aktualizacji poprawek popularnego oprogramowania pozwalają producentowi w dowolnym momencie dołączyć do aktualizowanego systemu funkcje, których działanie może być wymierzone przeciw interesom właściciela tego systemu.

Tradycyjnie te i podobne zagrożenia traktuje się jak „opowieści o żelaznym wilku". Należą do nich naprawdę poważne w skali kraju niebezpieczeństwa (wynikające z możliwości nadużyć przez firmy/instytucje domyślnie obdarzane zaufaniem) dla:

— dostawców oprogramowania, w szczególności oprogramowania powszechnie używanego i dokonującego samoaktualizacji (*autoupdate*);
— dostawców usług sieciowych (tu rośnie rola dostawców „chmur");
— dostawców sprzętu; ostatnio sporo słychać o możliwości zainstalowania nieznanego kodu we wszystkich procesorach i/lub chipsetach, np. w położonych w Azji fabrykach podzespołów[9];
— wystawców zaufanych podpisów SSL.

Znane są już przypadki naruszenia zaufania dla łańcucha dostaw aktualizacji — wycieki kluczy prywatnych zaufanych podpisów oprogramowania.

[8] W niniejszym tekście termin „antywirus" i jego pochodne używany jest jako nazwa handlowa produktów lub usług chroniących przed niepożądanym kodem (*malware*).

[9] Por. S. Anthony, *Rakshasa: The hardware backdoor that China could embed in every computer*. ExtremeTech 2012, <http://www.extremetech.com/computing/133773-rakshasa-the-hardware-backdoor-that-china-could-embed-in-every-computer>

Nie tylko dostawcy samoaktualizującego się oprogramowania lub zdobywcy zaufanych kluczy mogą zainstalować dowolne oprogramowanie na komputerach ofiary. Możliwość taką uzyskują dostawcy niektórych zapór sieciowych, odszyfrowujących ruch sieciowy dzięki wprowadzeniu własnych kluczy do magazynów certyfikatów zaufanych (używając nomenklatury Windows) stacji roboczych. Jest to rodzaj legalnego użycia MITM (ang. *man in the middle* — znanej techniki wykorzystywanej w atakach), chociaż nie zawsze za wiedzą poszczególnych użytkowników.

4. Wybrane cechy incydentów

Na początku roku 2015, jak zwykle o tej porze, opublikowano raporty znaczących firm dotyczące incydentów w obszarze bezpieczeństwa teleinformatycznego (CERT.gov[10], HP[11], TrendMicro[12] i Verizon[13]). Uważna lektura tych pozycji pozwala zauważyć prawidłowości istotne dla rozważań w zakresie ataków ukierunkowanych. W szczególności raport Verizon „2015 Data Breach Investigations Report" (tzw. DBIR[14]) jest interesujący, ze względu na obszerność materiału źródłowego obejmującego:

— 70 organizacji;
— 79 790 incydentów w obszarze bezpieczeństwa;
— 2122 udokumentowane naruszenia atrybutów bezpieczeństwa informacji (*data breaches*);
— 61 krajów (niestety, bez Polski)

oraz ogólną poprawność metodologiczną.

Cele ataków, to firmy i organizacje, które w znacznej części w Polsce zostałyby zaliczone do infrastruktury krytycznej (cyt. DBIR: „The top three industries affected are the same as previous years: Public, Technology/Information, and Financial Services").

Interesującym spostrzeżeniem jest to, że niektóre z nich nie były celem pierwszoplanowym, a były tylko środkiem lub etapem pośrednim do właściwego celu (cyt. DBIR: „In 70% of the attacks where we know the motive for the attack, there's a secondary victim"). To oznacza, że ataki były co najmniej dwuetapowe.

Nie jest zaskoczeniem, że czasy trwania poszczególnych ataków były krótsze, niż zdolność reakcji ludzi (cyt. DBIR: „In 60% of cases, attackers are able

[10] *Ataki ukierunkowane na instytucje administracji publicznej*. Wiadomości <Cert.gov.pl>, <http://www.cert.gov.pl/cer/wiadomosci/zagrozenia-i-podatnosc/118,dok.html>.

[11] *Cyber Risk Report 2015,* HP Security Research. HP 2015.

[12] R. Janicki, *Wprowadzenie do systemów IDS*. Sekurak, 23 marca 2015, <http://sekurak.pl/wprowadzenie-do-systemow-ids/>.

[13] Verizon. *2015 Data Breach Investigations Report*. Verizon 2015, <http://www.verizonenterprise.com/DBIR/2015/>.

[14] Tamże.