stosunkowo szybko zorientuje się, że ma do czynienia z fałszywym systemem to jednak takie rozwiązanie w znaczący sposób wyklucza ataki automatyczne i wywołane przez script-kiddies (hakerów amatorów) co w znaczny sposób pozwala odsiać nadmierny ruch oraz komunikaty typu false-positive z firewalla. Przede wszystkim warto pamiętać, że proporcjonalnie do tego ile autor rozwiązania włoży wysiłku i zaangażowania w konfigurację i ukrycie farmy, tyle dostanie czasu na możliwą reakcję i ocenę rodzaju i powagi zaobserwowanego zagrożenia lub incydentu. Wartością dodaną rozwiązania jest fakt, że honey-pot stanowi podstawową i aktualną bazę wiedzy w jaki sposób system jest atakowany co daje możliwość zabezpieczenia chronionego systemu przed zaobserwowanymi technikami ataku. Przedstawione w niniejszym artykule statystyki wskazują, że trend prób włamań na typowe dane i usługi, pomimo nieustannego uszczelniania systemów, cały czas utrzymuje się na podobnym poziomie. Dopóki świadomość administratorów i użytkowników nie zostanie zwiększona w zakresie zabezpieczania samych siebie i urządzeń na których pracują dopóty wyszukiwarki typu shodan (http://shodanhq.com) będą gromadziły dane o podatnych urządzeniach, które mogły być skutecznie zabezpieczone po włożeniu niewielkiego wkładu własnego w konfigurację.

W serwisie YouTube, pod adresem wskazanym w bibliografii: [9], autorzy niniejszej publikacji zamieszczają film prezentujący pełną instalację środowiska - oraz - obserwację pierwszej próby włamania i poczynań napastnika.

Literatura

[1] CERT: Raport Roczny z Działalności CERT Polska, ISSN 2084-9079, Warszawa, 2016

[2] http://www.cert.pl

[3] Redmiles E.: Why Installing Software Updates makes us WannaCry, The Conversion US, Scientific American, 2017

[4] Mansfield-Devine S.: Hacking on an industrial scale, Network Security, Elsevier, Issue 9, 2014, Str. 12-16

[5] Wang J., Zeng J.: Construction of large-scale honeynet based on Honeyd, Procedia Engineering, Elsevier, Volume 15, 2011, Str. 3260-3264

[6] Weiner K., Chelst K., Hart W.: Stinging the Detroit criminal: A total system perspective, Journal of Criminal Justice, Elsevier, Issue 3, Volume 12, 1984, Str. 289-302

[7] Adi K., Hamza L., Pene L.: Automatic security policy enforcement in computer systems, Computes and Security, Elsevier, Volume 73, 2018, Str. 156-171

[8] Pandya P.: TCP/IP Packet Analysis, Computer and Information Security Handbook (Second Edition), Morgan Kaufmann, 2013, Str. 499-512

[9] https://www.youtube.com/watch?v=v9kseYy5SII

Dr inż. Michał Podpora, mgr inż. Tomasz Turba, mgr inż. Agnieszka Różańska, dr inż. Aleksandra Kawala-Janik,
Politechnika Opolska

Przegląd zagadnień i zmian związanych z wdrożeniem w życie dyrektywy RODO/GDRP

Ochrona danych osobowych jest zagadnieniem, które w branży energetyki pozornie powinno interesować jedynie podmioty zajmujące się dystrybucją i sprzedażą energii. Pozornie, ponieważ dyrektywa RODO reguluje znacznie więcej niż dotychczasowe przepisy z 1995 r., wprowadzając zupełnie nowe podejście w zakresie prywatności, ochrony danych osobowych i bezpieczeństwa systemów informatycznych. Rozporządzenie RODO przez wielu przedsiębiorców jest uważane za niejasne i nie zawierające konkretnych zaleceń - m.in. ze względu na to, by najnowsze przepisy były jak najmniej zależne od ciągle postępującego rozwoju technologicznego, a także od specyfiki przetwarzania danych w danym przedsiębiorstwie. W niniejszym artykule autorzy postarają się przedstawić zarówno wybrane elementy dyrektywy, jak również ogólną techniczną koncepcję bezpieczeństwa systemów informatycznych - w odniesieniu do specyfiki branży energetycznej.

Wstęp

Europejska reforma ochrony danych osobowych, zwana potocznie jako reforma RODO [1], zaczyna obowiązywać od dnia 25 maja 2018 r. Dyrektywa ta ma za zadanie unowocześnienie regulacji o ochronie danych osobowych, gdyż poprzednie rozporządzenie, obowiązujące od 1995 r., ma coraz mniejsze zastosowanie praktyczne z powodu postępującej cyfryzacji.

Rozporządzenie RODO wnosi szereg zmian w regulacjach o ochronie danych osobowych. Jedną z ważniejszych zmian jest przenoszenie danych - każdy obywatel ma prawo wystąpić do przedsiębiorcy z żądaniem przekazania mu pliku w formacie *.pdf wraz z informacjami, jakie dane dotyczące jego osoby są wykorzystywane w tej firmie. Pozwoli to na łatwą kontrolę danych jakie są udostępniane między firmami i dzięki temu będzie można łatwiej kontrolować co będzie działo się z danymi osobowymi przetwarzanymi przez dany podmiot.

Trudności we wdrożeniu i utrzymaniu

Głównym zadaniem administratora danych osobowych ma być bezwzględne dostosowanie Systemów Informatycznych (SI) tak, aby dokładając wszelkiej staranności kontrolować te dane w sposób rzetelny i stabilny. W razie powstania żądania osób, których dane dotyczą - aby można było je w sposób kontrolowany i bezpieczny m.in. usunąć lub przekazać do innego usługodawcy. Wraz z wprowadzeniem w życie RODO powstaje również obowiązek udzielenia wszelkich informacji na temat danych osobowych zainteresowanego podmiotu oraz udzielenia mu odpowiedzi w terminie 30 dni od daty złożenia zapytania. W łatwy sposób można sobie wyobrazić paraliż instytucji publicz-

nej do której przyszła ogromna liczba zapytań od podmiotów na temat przetwarzania ich danych w przedsiębiorstwie. Podmiot zainteresowany swoimi danymi osobowymi będzie mógł wykorzystać „prawo do zapomnienia" [1] o nim w przedsiębiorstwie i poprosić o usunięcie jego danych osobowych z wszelkich nośników (systemy komputerowe, bazy danych, rejestry identyfikacji i dostępu, rejestry papierowe) w bardzo krótkim czasie. Może to oznaczać dodatkowy paraliż, któremu jednak można w łatwy sposób zaradzić - doprowadzić w przedsiębiorstwie do reengineeringu [2] przechodząc z dokumentacją osobową z postaci papierowej do cyfrowej. W przypadku naruszenia zasad bezpieczeństwa, przedsiębiorstwo ma bezwzględny nakaz zgłoszenia tego faktu w ciągu 72 h do organu nadzorującego. Powstaje więc pytanie co w przypadku, gdy luka w systemie istniała od tygodni, a naruszenie zostało wykryte dopiero teraz. Dyrektywa nie odpowiada na to pytanie w aktualnej wersji, ale podkreśla jasno, że bezpośrednia odpowiedzialność za naruszenie danych spada na przetwarzającego. Problemem jest także znany wymiar kar [3, 4], ale w wartości maksymalnej, która wynosi odpowiednio:

- 10 mln EURO lub 2% rocznego światowego obrotu firmy,
- 20 mln EURO lub 4% rocznego światowego obrotu firmy,
- 100 tys PLN karty administracyjnej za naruszenie ochrony danych osobowych przez administrację publiczną.

W/w wartości są wartościami maksymalnymi i wiadome jest, że zakres będzie proporcjonalny do naruszenia. Jednakże nie ma jasnych przykładów obrazujących przykładowo, że za nieusunięcie rekordu o Janie Kowalskim w bazie internetowej zostanie nałożona kara w zakresie od 100 PLN do 10 000 PLN. Ważnym aspektem i pierwszym punktem rozwoju i wdrożenia dyrektywy RODO w przedsiębiorstwie natomiast powinno być dostosowanie formularzy do zgody podmiotu na przetwarzanie jego danych oraz wskazanie zasadności takiego postępowania.

Podsumowanie

Dla przeciętnego Kowalskiego dzień wprowadzenia dyrektywy RODO nie będzie dniem przełomowym, choć owszem ułatwi mu walkę z podmiotami bezprawnie posiadającymi lub przekazującymi jego dane.

Natomiast dla przedsiębiorców, organizacji i innych podmiotów, dyrektywa RODO oznacza rewolucję w podejściu do danych osobowych i realną troskę o ich bezpieczeństwo. Co prawda dyrektywa nie opisuje wprost technologii które należy zastosować ani nawet koncepcji bezpieczeństwa, którą należy przyjąć - wielu przedsiębiorców i praktyków mówi wprost, że zapisy dyrektywy są pod względem technicznym niejasne [4], jednak jej autorzy i również komentatorzy wyjaśniają, że jest to zabieg celowy, nakłaniający podmioty do dogłębnego przeanalizowania środków technicznych i procedur dotyczących przechowywania i przetwarzania danych i zaprojektowania [4] własnego rozwiązania.

Jak na razie za wcześnie jest by widzieć kompletny bilans zysków i strat wynikający ze zmiany przepisów. Każda zmiana wprowadzana jest w nadziei na polepszenie sytuacji, a sytuacja związana z ochroną danych osobowych od wielu lat nie ulegała zmianom.

Niestety jak na razie niejasne [4] zapisy RODO nie pomagają przedsiębiorcom w odnalezieniu się w nowej rzeczywistości, wizja potężnych kar [3, 4] również wprowadza atmosferę niepewności, spekulacje dotyczące zakresu ochrony (np. czy pliki cookies podlegają pod zapisy RODO [4]) także podgrzewają atmosferę w niejednej firmie. Nawet firmy nie zajmujące się zagadnieniami informatycznymi, posiadające jedynie stronę internetową, często z zaniepokojeniem obserwują zamęt choćby wokół marketingu internetowego [4, 5].

Wspomniana atmosfera niepokoju i dbałość o dostateczne wypełnienie przepisów, czasem doprowadza do działań o negatywnych marketingowo skutkach, jak miało to miejsce w przypadku firmy Tauron Polska Energia, która, zapewne z dbałości o dobrowolność i świadomość faktu przetwarzania danych danego klienta przez tą firmę, poprosiła klientów o zgodę, co przez znaczną część społeczeństwa zostało odebrane zdecydowanie negatywnie (zarówno w mediach społecznościowych [6], jak i na portalach branżowych z zakresu bezpieczeństwa [7]). Tak więc na razie przed nami trudny okres przejściowy, w którym nie tyle przepisy ulegają zmianie, co świadomość przedsiębiorców ale i wszystkich użytkowników globalnej sieci.

Pozostaje mieć nadzieję, że podmioty dopuszczające się nadużyć w zakresie przetwarzania danych nie znajdą obejścia tych przepisów, lub obejście takie nie będzie opłacalne lub będzie zbyt ryzykowne. W przeciwnym wypadku cały trud związany z realizacją RODO mógłby się stać tylko biurokratyczną komplikacją i kolejną stertą formularzy, zniechęcającą klientów do korzystania z usług podmiotu.

Literetura

[1] Generalny Inspektor Danych Osobowych: Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)., dostęp on-line (2018-01-01): http://www.giodo.gov.pl/pl/569/9276

[2] Pattanayak S., Roy.: Synergizing Business Process Reengineering with Enterprise Resource Planning System in Capital Goods Industry, Procedia - Social and Behavioral Sciences, Volume 189, 2015, Str. 471-487

[3] Business Insider Polska: Kto się boi reformy RODO? Działy IT czeka duża zmiana., 2017-12-18, dostęp on-line (2018-01-02): https://businessinsider.com.pl/firmy/rodo-zmiany -w-prawie-ochrony-danych-osobowych-w-ue/y1b3nf4

[4] Maroszek W.: RODO, czyli ochrona danych 2.0. Nowe unijne przepisy oznaczają trudności dla przedsiębiorców., Business Insider Polska, 2018-01-09, dostęp on-line (2018-01-10): https://businessinsider.com.pl/firmy/przepisy/rodo-gdpr-regulacje-o-ochronie- danych-osobowych-zmiany-w-firmach/21p6svs

[5] Odo24.pl: Strefa RODO - najważniejsze zmiany i nowości, ODO24, 2018, dostęp on-line (2018-01-20): https://odo24.pl/rodo

[6] Oficjalny profil TAURON Polska Energia: posty internautów pod komunikatami i materiałami marketingowymi w okolicach 20 stycznia 2018, dostęp on-line (2018-01-22): https://www.facebook.com/pg/tauronpolskaenergia/posts/

[7] Maj M.: Dokładnie przeczytajcie pismo, jakie przesłał wam i waszym rodzicom Tauron, Niebezpiecznik.pl, 2018-01-09, dostęp on-line (2018-01-15): https://niebezpiecznik.pl/post/tauron-stosuje-sprytna-socjotechnike-by-pozyskac-zgody-marketingowe/