dr inż. GRZEGORZ OWCZAREK
Centralny Instytut Ochrony Pracy
– Państwowy Instytut Badawczy
Kontakt: growc@ciop.lodz.pl
dr inż. ARTUR HŁOBAŻ
Uniwersytet Łódzki, Wydział Fizyki i Informatyki Stosowanej
Kontakt: artur.hlobaz@uni.lodz.pl
DOI: 10.5604/01.3001.0013.0255

Bezpieczeństwo teleinformatyczne w systemach przemysłowego Internetu rzeczy na przykładzie środowiska pracy

Fot. Lichtmeister/Bigstockphoto

W artykule omówiono powody, dla których konieczne jest zapewnienie bezpieczeństwa obiegu danych i informacji w systemach przemysłowego Internetu rzeczy (IoT). Zaprezentowano warstwową architekturę bezpieczeństwa wraz z elementami zabezpieczenia poszczególnych warstw. Obieg danych i informacji zbieranych i przetwarzanych w strukturach Internetu rzeczy w środowisku pracy zilustrowano przykładem systemu, w skład którego wchodzą czujniki zintegrowane ze środkami ochrony indywidualnej. Zaprezentowano również ogólne zasady, jakimi należy się kierować przy wprowadzaniu dobrych praktyk w zakresie zapewnienia bezpieczeństwa obiegu danych i informacji.

Słowa kluczowe: bezpieczeństwo teleinformatyczne, Internet rzeczy, środowisko pracy, środki ochrony indywidualnej

ICT security in industrial Internet of things systems on the example of the work environment

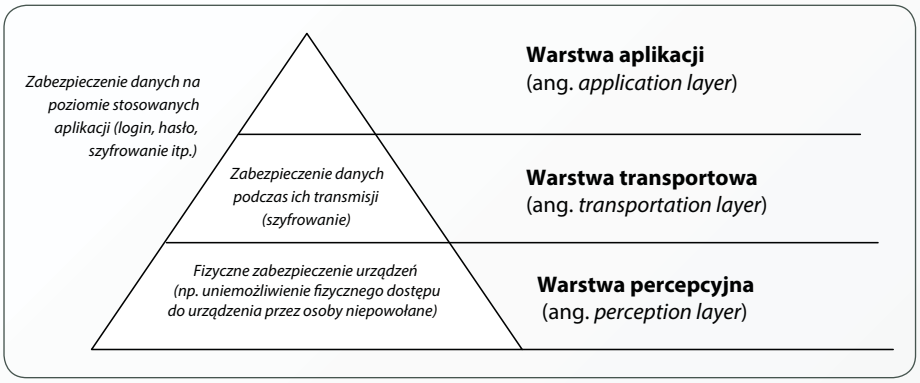
The starting point of this article is the presentation of knowledge transfer as one of the most important elements in respect to the organization functioning in a world of knowledge-based economy and knowledge-based processes.
The article discusses the reasons why it is necessary to ensure the security of the data and information flow in the Industrial Internet of Things (IoT) and its systems. A layered security architecture with elements of protection of particular layers was presented. The flow of data and information collected and processed in the Internet of Things structures in the work environment is illustrated by an example of a system that includes sensors integrated with personal protective equipment. The article also presents general principles that should be followed when developing good practices in the area of ensuring the security of data and information flow.

Keywords: IST security, Internet of Things, working environment, personal protective equipment

Wstęp

Zagadnienie bezpieczeństwa teleinformatycznego i ochrony danych dotyczy wielu obszarów, w tym również środowiska pracy. Wynika to ze zmian, które obecnie zachodzą na wielu stanowiskach pracy. Zmiany te są porównywane do tych, które zachodziły na początku XIX w., zwanego wiekiem pary i elektryczności (tzw. druga rewolucja przemysłowa). To, co określamy obecnie jako czwartą rewolucję przemysłową (*Industry 4.0*) jest naturalną kontynuacją ciągłego postępu w dziedzinie nauki i techniki. Lata 50. XX w. uważa się za początek tzw. trzeciej rewolucji przemysłowej, czyli przemysłu opartego na automatyzacji i komputeryzacji procesów produkcyjnych. Było to możliwe dzięki wynalazkom, takim jak krzemowe elementy półprzewodnikowe (tranzystory, układy scalone), światłowody, materiały syntetyczne i kompozytowe oraz nowym źródłom energii (m.in. energetyce jądrowej). Wszystko to w znaczący sposób zmieniło sposób funkcjonowania środowiska pracy. Trzecia rewolucja przemysłowa trwa do dziś.

Czwarta rewolucja przemysłowa to zastosowanie technologii cyfrowych w środowisku pracy. *Industry 4.0* oznacza bowiem zespół zaawansowanych technologii i zasad funkcjonowania systemów produkcji z wykorzystaniem systemów cyber-fizycznych oraz systemów komunikacji, przyjmujących za podstawę koncepcję Internetu rzeczy (*Internet of Things*, IoT) oraz przetwarzania chmurowego. Transformacja określana mianem 4.0 odnosi się do procesorowego przetwarzania i interpretowania informacji pobranych przez sensory. Charakteryzuje się ono trzema podstawowymi cechami: działaniem w czasie rzeczywistym, realizacją programową przetwarzania zapew-



Rys. 1. Architektura bezpieczeństwa stosowana dla zabezpieczenia systemów IoT i elementy zabezpieczenia poszczególnych warstw

Fig.1. Security architecture used to secure IoT systems and security elements of individual layers

niającą zdolność kształtowania właściwości i zachowań mechatronicznego systemu produktu oraz osiągnięciem takiego stopnia inteligencji maszynowej, który pozwala na przejęcie od użytkownika produktu przynajmniej części odpowiedzialności za realizację przewidzianych działań [2].

W procesach produkcyjnych stosowane są coraz częściej nowoczesne technologie informacyjne (*Information Technology,* IT). Wraz ze zmianami zachodzącymi w środowisku pracy – określanym coraz częściej jako inteligentne – pojawiły się nowe wyzwania dla architektów je projektujących [2]. Jest to środowisko, które stanowi ogólnie pojętą cyberprzestrzeń, czyli miejsce do przetwarzania i wymiany danych i informacji, utworzonych przez systemy teleinformatyczne [3].

Zagadnienie obiegu danych i informacji w kontekście bezpieczeństwa teleinformatycznego nabiera całkiem innego wymiaru, gdy mamy do czynienia z danymi lub informacjami, które mogą zaistnieć w przestrzeni internetowej. Do najważniejszych zagrożeń z tym związanych należy zaliczyć: niedostępność usług, ryzyko integralności danych, uzależnienie od dostawcy chmury obliczeniowej, niepowołany dostęp i poufność danych, czy niewystarczające uregulowania prawne [4].

Pisząc o obiegu danych i informacji w różnego rodzaju systemach elektronicznych należałoby wstępnie określić, co kryje się pod pojęciem „dane" [5]. Należy przez to rozumieć dane, które przygotowuje się w celu przetworzenia, przechowywania lub przesyłania, czyli różnego typu pliki lub strumienie danych multimedialnych (np. VOD, *Video on Demand*), radio internetowe), dane pomiarowe z czujników, dane uwierzytelniające (login i hasło). Z punktu widzenia przechowywania oraz przesyłania danych przez sieć komputerową stanowią one ciąg bitów. Dopiero na poziomie warstwy aplikacji ciąg ten interpretowany jest ze względu na zawartość, tzn. to, co reprezentuje i jakiego rodzaju są to dane [6].

Dane definiowane są również jako zbiory liczb i tekstów oraz grafik o różnych formach. Mogą więc mieć konkretną wartość informacyjną [7]. Semantyczna różnica pomiędzy pojęciami „dane" i „informacje" jest taka, że różne dane mogą dostarczać tych samych informacji, ale jednocześnie te same dane mogą dostarczać różnych informacji [8]. Z uwagi na możliwości zróżnicowania pojęć „dane" i „informacje", w dalszej części artykułu stosowane jest wyłącznie określenie „dane" – z wyłączeniem części, w której opisano zbieranie i przetwarzanie danych i informacji w systemie funkcjonującym na bazie koncepcji Internetu rzeczy w środowisku pracy, określanego jako przemysłowy Internet rzeczy.

Celem artykułu jest zaprezentowanie koncepcyjnego sposobu na bezpieczny obieg danych i informacji zbieranych i przetwarzanych w systemach przemysłowego Internetu rzeczy w środowisku pracy.

Powody zapewniania ochrony danych

Jedną z najważniejszych przesłanek monitorowania bezpieczeństwa w obiegu danych i informacji w cyberprzestrzeni są ataki hakerskie. Cyberprzestrzeń – w tym również środowiska pracy – podlega ciągłemu narażeniu na ingerencję osób nieuprawnionych [9]. Problem ten jest obecnie również zagadnieniem szeroko dyskutowanym pod kątem zachowań społecznych.

Haker to osoba należąca do swoistej subkultury, zazwyczaj o bardzo dużej wiedzy i umiejętnościach z zakresu systemów informatycznych, które to umiejętności są wykorzystywane do łamania zabezpieczeń systemów komputerowych. Jeśli podczas ataków hakerskich zostaną przechwycone dane o charakterze wrażliwym, które następnie będą wykorzystane niezgodnie z intencjami osób, których dotyczą, może to być powodem wielu zdarzeń o nie do końca przewidywalnych następstwach. Mogą to być skutki ekonomiczne, prawne lub osobowe, związane choćby z narażeniem konkretnej osoby na ujawnienie w przestrzeni publicznej informacji o jej stanie zdrowia. Kolejnym, nie mniej ważnym powodem, dla którego konieczne jest monitorowanie bezpieczeństwa danych, są wymogi prawne.

W ramach reformy systemu ochrony danych osobowych w Unii Europejskiej przyjęto rozporządzenie Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych [10] Nowe rozporządzenie obowiązuje we wszystkich krajach Unii Europejskiej – w Polsce od 25 maja 2018 r. Ochrona danych dotyczy w sposób szczególny danych, które są określane jako dane osobowe i przysługuje każdemu obywatelowi. Zgodnie z nowym rozporządzeniem dane osobowe oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"). Oznacza to, że można ją bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie imienia i nazwiska, numeru identyfikacyjnego, danych o lokalizacji, identyfikatora internetowego lub jednego/kilku szczególnych czynników, określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

Główną przyczyną zmiany przepisów w zakresie ochrony danych osobowych jest działalność globalnych firm, takich jak Google, Facebook lub Apple, zarządzających ogromną ilością danych (i je przetwarzających), wśród których są również dane osobowe o charakterze wrażliwym. Firmy te nie podlegały bezpośrednio wycofanej dyrektywie 95/46/WE [11].

Świadomość zagrożenia, jakie może stwarzać niczym niekontrolowany sposób przetwarzania danych osobowych sprawia, że niektóre korporacje inicjują również własne działania w zakresie ochrony danych osobowych. Generuje to jednak koszty i nie zapewnia wymaganego poziomu bezpieczeństwa w zakresie ochrony danych o charakterze wrażliwym. Przykładem istotnych braków w zakresie monitorowania bezpieczeństwa danych była głośna afera związana z wyciekiem danych z najbardziej popularnego serwisu społecznościowego[1].

Ochrona danych jest również obecnie ważnym elementem środowiska pracy.

W ostatnich latach pojawiają się również tzw. inteligentne środki ochrony indywidualnej. Są to wyroby, w których zaimplementowane zostały mikro-elektromechaniczne układy zapewniające dodatkowe, specyficzne funkcje, takie jak monitorowanie zagrożeń środowiskowych oraz wybranych parametrów fizjologicznych użytkowników.

[1] W marcu 2018 r. miała miejsce głośna afera związana z firmą Cambridge Analytica i Facebookiem. Z doniesień medialnych wynikało, że wyciekły dane nawet 50 mln użytkowników Facebooka na całym świecie.

Obieg danych i bezpieczeństwo przemysłowego Internetu rzeczy

Obieg danych we wszystkich systemach elektronicznych i telekomunikacyjnych, bankowych itp., a także w Internecie rzeczy (IoT), opiera się na trzech podstawowych elementach: integralności, poufności i dostępności.

Integralność oznacza, że dane są kompletne i zebrane z wystarczającą dokładnością, aby wygenerować informacje, które chcemy otrzymać. Należy również zapewnić odpowiednie metody przetwarzania tych danych. Poufność oznacza, że zbierane dane/informacje są dostępne jedynie dla osób do tego upoważnionych. Dostępność to zapewnienie osobom upoważnionym dostępu do danych/informacji zawsze, gdy jest taka potrzeba [12].

Najlepszą metodą zabezpieczenia danych jest metoda wielopoziomowa, w której rozpoczynamy od bezpieczeństwa fizycznego, a kończymy na warstwie aplikacji. Jest to więc zabezpieczenie danych zarówno przed kradzieżą nośników danych, jak i przed wszelkimi atakami hakerskimi oraz dostępem niepowołanych osób do urządzeń, na których uruchomione są aplikacje. Ogólny schemat architektury bezpieczeństwa, która może być zastosowana dla wszystkich systemów w obszarze IoT może składać się z trzech podstawowych warstw [13]: percepcyjnej, transportowej i aplikacji (rys. 1., s. 9.)

Na każdej z warstw przedstawionych na rys. 1. zabezpieczanie danych może odbywać się niezależnie. Ta niezależność jest niezmiernie istotna z punktu widzenia bezpieczeństwa całego systemu [14]. Przykładowo, jeśli dane zabezpieczone będą tylko podczas transmisji (w warstwie transportowej), nadal teoretycznie pozostaje możliwość uzyskania do nich dostępu za pomocą niezabezpieczonego urządzenia (brak zabezpieczenia w warstwie aplikacji na poziomie laptopa lub smartfona, chociaż jest to stosunkowo rzadka sytuacja). Podobnie jest również w drugą stronę: jeśli dostęp do danych zgromadzonych w danym urządzeniu będzie zabezpieczony (w warstwie aplikacyjnej), to można do nich uzyskać dostęp, jeżeli są przesyłane w postaci niezaszyfrowanej (brak zabezpieczenia w warstwie transportowej).

Możliwe jest bardziej szczegółowe rozdzielenie poszczególnych warstw, tak aby wyodrębnić najważniejsze elementy wchodzące w skład danego systemu. Przykładem jest struktura pięciowarstwowa, składająca się z warstw [15]:

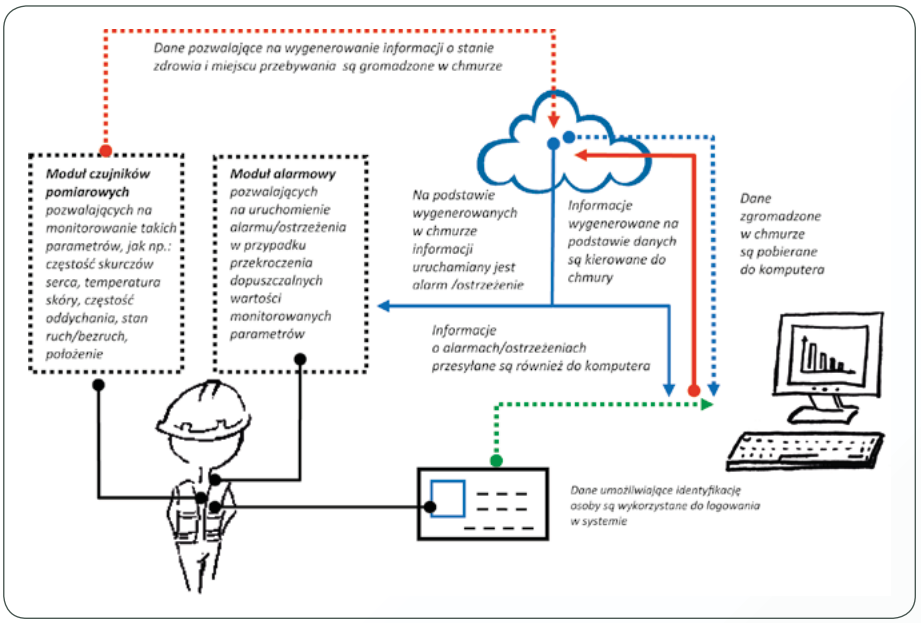
– percepcyjnej (*perception layer*)

– bezpieczeństwa i kontekstu (*security and context layer*)

– sieciowej i transportowej (*network and transportation layer*)

– chmurowej (*cloud storage and mobility*)

– analitycznej (*analytical layer*).



Rys. 2. Koncepcja obiegu danych i informacji w systemie, w skład którego wchodzą czujniki zintegrowane ze środkami ochrony indywidualnej

Fig. 2. Diagram of an example of the data and information flow in the system, which includes sensors integrated with personal protective equipment

Warstwowa struktura bezpieczeństwa IoT jest w dużej mierze zbieżna ze standardem OSI (*Open Systems Interconnection Reference Model*), opisującym ogólną strukturę komunikacji sieciowej [16]. Standard ten składa się z siedmiu warstw: fizycznej, łącza danych, sieciowej, transportowej, sesji, prezentacji i aplikacji.

Przykład obiegu danych i informacji w środowisku pracy

Przykład obiegu danych i informacji w środowisku pracy dotyczy koncepcji systemu, w skład którego wchodzą czujniki zintegrowane ze środkami ochrony indywidualnej (ŚOI). W zagadnieniu monitorowania parametrów środowiska pracy i stanu zdrowia pracowników systemy tego typu mają kluczowe znaczenie. Tylko w nielicznych przypadkach mogą to być gotowe systemy, możliwe do bezpośredniego zaadoptowania w dowolnym środowisku pracy. W sposób szczególny dotyczy to właśnie rozwiązań, w których czujniki są zaimplementowane w ŚOI [17]. Przykładem takiego rozwiązania jest system monitorowana wybranych parametrów środowiska pracy i parametrów fizjologicznych, zaimplementowany do odzieży strażackiej [18].

Konstrukcje czujników monitorujących parametry środowiska pracy oraz fizjologiczne są nieustannie rozwijane. Dotyczy to zarówno samej miniaturyzacji, jak i możliwości bezpośredniej integracji czujników o elastycznych podłożach z elementami odzieży ochronnej [19].

W celu przeanalizowania obiegu danych i informacji w środowisku pracy posłużono się koncepcją systemu (rys. 2.), w skład którego wchodzą czujniki zintegrowane ze środkami ochrony indywidualnej. System ten składa się z następujących elementów:

– identyfikatora elektronicznego w formie karty chip

– modułu czujników pomiarowych zintegrowanych z elementami środków ochrony indywidualnej, pozwalających na monitorowanie takich parametrów, jak częstość skurczów serca, temperatura skóry, częstość oddychania, stan ruch/bezruch, położenie

– komputera z oprogramowaniem obsługującym system

– modułu alarmowego (dla powiadomienia użytkownika o zagrożeniu zdrowia lub zabronionej lokalizacji)

– chmury obliczeniowej.

W tym przykładzie użytkownik ma identyfikator elektroniczny w formie karty chip z danymi, umożliwiającymi jego identyfikację. Aby system zaczął działać, użytkownik musi się zalogować, używając identyfikatora, na którym są zapisane takie dane, jak imię i nazwisko, stopień, funkcja itp. Po zalogowaniu oprogramowanie obsługujące system umożliwi skorelowanie pozostałych danych, otrzymywanych z czujników, z określoną osobą. Dane z czujników do monitorowania stanu zdrowia i położenia są przesyłane do chmury obliczeniowej, co jest możliwe dzięki zastosowaniu modułów elektronicznych, umożliwiających transmisję danych w trybie *on line*.

W chmurze dane są przetwarzane z wykorzystaniem aplikacji przeznaczonych do obsługi konkretnego systemu. Z tego względu preferowana jest konfiguracja tzw. chmury prywatnej. Czujniki należy w tym przypadku rozumieć jako

urządzenia, w skład których wchodzą zarówno elementy sensoryczne, jak i układy pozwalające na transmisję danych [1]. Dane te są w następnej kolejności przesyłane do komputera z oprogramowaniem obsługującym system. Zawiera ono również aplikacje pozwalające na wygenerowanie informacji o stanie zdrowia i położeniu użytkownika, które są następnie kierowane ponownie do chmury obliczeniowej, skąd mogą być wysłane w formie alarmu (jeśli wystąpi zagrożenie zdrowia lub użytkownik znajdzie się w zabronionej lokalizacji) do użytkownika. Informacje o alarmach przesyłane są także do komputera, w którym zapisywana jest historia uruchamianych alarmów.

Dane mogą być również gromadzone w identyfikatorze oraz w modułach elektronicznych, które umożliwiają transmisję danych w trybie *on line* do chmury obliczeniowej. Zakładając, że identyfikator elektroniczny jest czymś w rodzaju dowodu osobistego, bezpieczeństwo zapisanych na nim danych zależy od samego użytkownika. Musi on zdawać sobie sprawę, że w przypadku zagubienia lub nieuprawnionego użyczenia identyfikatora, nieupoważniona osoba może zalogować się do systemu. W przypadku modułów elektronicznych umożliwiających transmisję danych do chmury obliczeniowej zalecane jest, aby nie zapisywały one danych, zwłaszcza osobowych (ze względów bezpieczeństwa). Moduł elektroniczny umożliwiający transmisję danych do chmury obliczeniowej jest zwykle zintegrowany z środkiem ochrony indywidualnej. Może to być integracja stała, choć w większości przypadków moduły takie są dołączane do poszczególnych czujników i chowane w specjalnie zaprojektowanej do tego celu kieszeni. Jeśli więc dane, otrzymane w wyniku monitorowania parametrów fizjologicznych człowieka (które są danymi osobowymi), byłyby zapisywane i przechowywane w sposób trwały, istniałoby ryzyko dostępu do tych danych przez nieuprawnione osoby (np. obsługa magazynu, pralni).

Z przytoczonego wcześniej przykładu obiegu danych i informacji w koncepcyjnym systemie, w skład którego wchodzą czujniki zintegrowane z ŚOI, wynika, że aby zapewnić ich bezpieczeństwo, konieczne jest niezależne zabezpieczenie trzech warstw, wchodzących w skład opisanej wcześniej architektury bezpieczeństwa. W warstwie percepcyjnej jest to zabezpieczenie dostępu przez osoby nieuprawnione do wszystkich elementów fizycznych systemu pokazanego na rys. 2., czyli do komputera, identyfikatora elektronicznego i czujników. W warstwie transportowej zabezpieczenie danych i informacji polegać będzie na szyfrowaniu przepływu danych i informacji we wszystkich opisanych kierunkach przepływu. Zabezpieczenie w warstwie aplikacji polega na szyfrowanym dostępie do wszystkich aplikacji dostępnych w chmurze i na komputerze.

Dobre praktyki w zakresie zapewnienia bezpieczeństwa obiegu danych i informacji

Zapewnienie bezpieczeństwa obiegu danych i informacji powinno obejmować wszystkie wymienione elementy. W odniesieniu do warstwy percepcyjnej są to głównie zastosowane czujniki, aktuatory itp., a w stosunku do warstwy transportowej monitorowaniem bezpieczeństwa powinny zostać objęte technologie transmisji danych. W kontekście warstwy aplikacji są to wszelkie algorytmy i aplikacje pozwalające na gromadzenie, przetwarzanie i dostęp do danych.

Monitorowanie integralności to głównie nadzór nad jakością danych. Monitorowanie poufności polega na śledzeniu okoliczności, w których poufność nie została zachowana oraz przewidywaniu sytuacji, w których może dojść do jej naruszenia. W tym celu śledzone są działania użytkowników systemów zawierających dane, co polegać może m.in. na rejestracji kierunków ich transferu oraz sposobu, w jaki zastosowane w systemie algorytmy i aplikacje są wykorzystywane przez użytkowników. Monitorowanie dostępności polega na nadzorowaniu korzystania z infrastruktury technicznej oraz oprogramowania, badaniu parametrów określających wydajność i obciążenie systemu, a także sprawdzaniu kompatybilności z innymi współpracującymi systemami. Wszystkie chcące uniknąć cyberataków instytucje, w których funkcjonują systemy elektroniczne i telekomunikacyjne, powinny zweryfikować, w jaki sposób urządzenia działające na bazie IoT są wdrażane i zabezpieczane [20].

W listopadzie 2017 r. European Union Agency for Network and Information Security opublikowała dokument, skupiający się na najważniejszych elementach związanych z cyberbezpieczeństwem w systemach IoT i określeniu podstawowych zaleceń z nim związanych [21]. Poniżej wyszczególniono najważniejsze zawarte w nim rekomendacje:

– częsta aktualizacja oprogramowania urządzeń

– częsta zmiana domyślnych danych uwierzytelniających (haseł) i ustawień urządzeń

– wybieranie wystarczająco skomplikowanych haseł

– prawidłowa konfiguracja zapory (*firewall*) i odfiltrowywanie/blokowanie podejrzanego ruchu

– odpowiednie śledzenie i zarządzanie urządzeniami – dobrym punktem wyjścia do projektowania IoT jest dokładne zrozumienie, jak są połączone urządzenia, w związku z czym zaleca się wdrożenie rozwiązania wykrywania, śledzenia i zarządzania zasobami

– fizyczne zabezpieczanie urządzeń pośrednich w transmisji przed dostępem np. routerów lub switchy

– wykonanie testów penetracyjnych lub oceny urządzeń na poziomie sprzętu lub oprogramowania przed ich wdrożeniem, w celu wykrycia luk w zabezpieczeniach

– stosowanie aktualnych protokołów szyfrowania

– zabezpieczenie całej transmisji danych najlepiej na poziomie warstwy transportowej jak i warstwy aplikacji

– zabezpieczenie/szyfrowanie danych przechowywanych zarówno na urządzeniach końcowych jak i serwerach

– przejście od kontroli na poziomie urządzenia do kontroli na poziomie tożsamości

– ograniczenia związane z gromadzeniem danych – zbieranie tylko danych potrzebnych do świadczenia usługi i przechowywanie ich jedynie przez ograniczony czas

– w przypadku transmisji bezprzewodowej ustawienie niezbędnego i wystarczającego poziomu mocy urządzeń, aby zasięg transmisji był pod kontrolą.

W celu zapewnienia bezpieczeństwa danych w sytuacji użytkowania przez pracowników inteligentnych ŚOI, niezmiernie istotne jest, aby pracodawca wypełnił następujące warunki:

– Zapewnienie wymogów prawnych. Procedury generowania, przechowywania i transmisji danych powinny być zgodne z obowiązującymi przepisami (RODO). Pracodawca powinien powołać administratora danych osobowych i wyznaczyć osoby odpowiedzialne za nadzór nad pracownikami wyposażonymi w inteligentne ŚOI oraz nadzór nad stanem technicznym całego systemu inteligentnych środków ochrony indywidualnej.

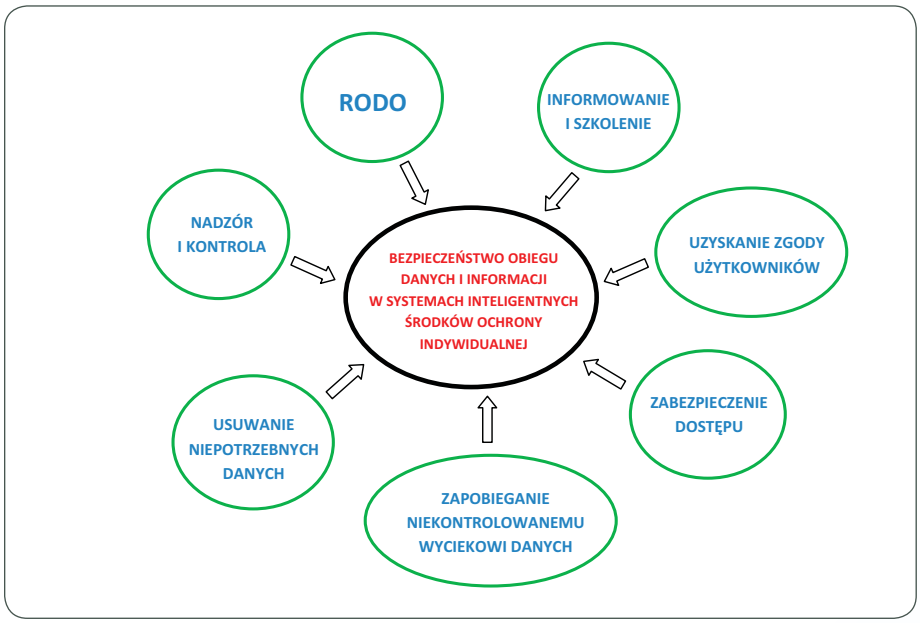
– Informowanie i szkolenie pracowników. Pracownicy użytkujący systemy inteligentnych ŚOI powinni zostać poinformowani o procedurze generowania, przechowywania i transmitowania danych i przeszkoleni w zakresie obsługi użytkowanych systemów inteligentnych ŚOI oraz procedur związanych z dostępnością do danych.

– Uzyskanie zgody pracowników. Pracownicy użytkujący inteligentne ŚOI muszą wyrazić zgodę na przetwarzanie ich danych osobowych.

– Zabezpieczenie dostępu. Dostęp do elementów systemu inteligentnych ŚOI mogą mieć wyłącznie osoby upoważnione.

– Zapobieganie niekontrolowanemu wyciekowi danych. Nie zaleca się wysyłania danych monitorowanych do serwerów pracodawcy lub rozwiązań chmurowych. Najlepiej, aby dane były rejestrowane lokalnie na urządzeniu stosowanym przez pracownika. Powinno się przesyłać dane tylko w uzasadnionych przypadkach. Pod żadnym pozorem nie należy umieszczać danych (w szczególności danych wrażliwych) na portalach społecznościowych.

– Usuwanie niepotrzebnych danych. Pod koniec pracy wszystkie niepotrzebne dane, które zostały zgromadzone podczas użyt-



Rys. 3. Elementy wpływające na poziom bezpieczeństwa obiegu danych i informacji generowanych, przechowywanych i transmitowanych w systemach inteligentnych ŚOI

Fig.3. Elements affecting on the security level of data flow and information generated, stored and transmitted in smart PPE systems

kowania inteligentnych ŚOI należy usunąć (najlepiej automatycznie).

– Kontrola i nadzór nad systemem. Sprawne działanie systemu inteligentnych ŚOI, zarówno w aspekcie technicznym (m.in. testy penetracyjne, kontrola czujników.), jak również pod kątem przestrzegania procedur związanych m.in. z weryfikacją haseł oraz osób upoważnionych do dostępu do poszczególnych elementów systemu, jest ważnym elementem bezpieczeństwa danych i informacji.

Na rys. 3. przedstawiono schematycznie wymienione elementy, których realizacja podnosi poziom bezpieczeństwa obiegu danych i informacji przechowywanych i transmitowanych w systemach inteligentnych ŚOI.

Podsumowanie

Brak zapewnienia prawidłowego obiegu danych uniemożliwia skuteczne zarządzanie ich bezpieczeństwem. Działania w tym zakresie powinny obejmować możliwie wszystkie aspekty, które mogą mieć znaczenie w odniesieniu do skutecznego zabezpieczenia danych i informacji przechowywanych i transmitowanych w systemach inteligentnych ŚOI. Dlatego też konieczne jest zastosowanie warstwowej architektury bezpieczeństwa, co wiąże się z wprowadzeniem niezależnych zabezpieczeń poszczególnych warstw (percepcyjnej, transportowej i warstwy aplikacji).

Nie bez znaczenia jest również zwrócenie uwagi na to, czy w samym procesie monitorowania bezpieczeństwa danych i informacji w kontekście inteligentnych ŚOI biorą udział osoby odpowiednie do tego typu zadań. Ten aspekt (społeczny) jest jednym z najtrudniejszych i najbardziej wrażliwych w całym procesie związanym z monitorowaniem bezpieczeństwa danych. Jak powiedział kiedyś jeden z najbardziej znanych hakerów Kevin Mitnick *nieważne, ile wydaje się na rozwiązania technologiczne. System bezpieczeństwa jest tak silny, jak jego najsłabsze ogniwo – człowiek*. To właśnie użytkownicy, administratorzy są najbardziej newralgicznym punktem infrastruktury IT. Nigdy nie można mieć pewności, że osoby odpowiedzialne za bezpieczeństwo danych, na określonych etapach gromadzenia, przetwarzania lub przesyłania, nie okażą się hakerami, dla których bezpośredni dostęp do procedur związanych z monitorowaniem bezpieczeństwa będzie tylko ułatwieniem procederu związanego np. z wyciekiem danych wrażliwych. Istotne jest więc również to, aby zapewnić takie procedury monitorowania bezpieczeństwa w systemie, aby mógł on również sam siebie monitorować [22].

Wszystkie opisane w artykule aspekty zapewniania bezpieczeństwa obiegu danych i informacji przechowywanych i transmitowanych w systemach inteligentnych ŚOI są na ogół sformalizowane i wdrażane na podstawie jasno określonej polityki bezpieczeństwa, która powstaje na podstawie norm i zaleceń (dobrych praktyk). Im dane mają być bardziej bezpieczne, tym bardziej rygorystyczna polityka bezpieczeństwa zostaje wprowadzona.

BIBLIOGRAFIA

[1] Ostalczyk P., Jezierski E., Gmyrek Z., Szczerbanowski R., Tosik G., Lisik Z., Gołębiewski J., Pacholski K., Gniotek, K., Frydrych I., Korycki R., Sobiczewska G., Dems, M., Wiak S., Rosiak W., Drzymała P., Welfle H., Lasota, R., Glaba M.J., *Mechatronika. Tom 2.* [w:] podręcznik pod red. Wiak S., wyd. EXIT, Politechnika Łódzka, Łodź 2010

[2] Owczarek G. *Wybór czujników do monitorowania parametrów środowiska pracy i stanu zdrowia pracowników.* Rozdział w monografii *Nowe trendy w bezpieczeństwie pracy, środowisku i zarządzaniu.* WSZOP 2018

[3] Polityka ochrony cyberprzestrzeni Rzeczpospolitej Polskiej, 2013 https://www.cert.gov.pl/cer/publikacje/polityka-ochrony-cyber/639,Polityka-Ochrony-Cyberprzestrzeni-Rzeczypospolitej-Polskiej.html [dostęp: 10 V 2018]

[4] Fulmański P., Wojczyk S. *Potencjalne korzyści i zagrożenia związane z chmurą obliczeniową.* Zeszyty Naukowe Uniwersytetu Szczecińskiego „Studia Informatica" 2014,798,34:33-44

[5] Na podstawie internetowego słownika pojęć technicznych „TechTerms": https://techterms.com/definition/data [dostęp: 10 V 2018]

[6] Na podstawie serwisu internetowego Computer Hope: https://www.computerhope.com/jargon/d/data.htm, [dostęp: 10 V 2018]

[7] Wilson G. *Przetwarzanie danych dla programistów.* Wydawnictwo HELION 2006

[8] Gadomski A. *Global TOGA Meta-Theory* 1989

[9] Mitnick K., Simon W.L., Wozniak S. *Ghost in the Wires. My Adventures as the World's Most Wanted Hacker.* Little, Brown and Company 2011

[10] 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. Dz.Urz. UE L 119/1 z 4 maja 2016

[11] Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych

[12] Stallings W. *Cryptography and Network Security: Principles and Practice.* Pearson Education Limited, 2016

[13] Qi Jing, Vasilakos A.V., Jiafu Wan, Jingwei Lu, Dechao Qiu, *Security of the Internet of Things: perspectives and challenges.* "Wireless Netw." 2014,20:2481-2501

[14] Surman G. *Understanding security using the OSI model.* SANS Institute, 2002

[15] *Why Industrial IoT platform is best hope for IT and OT convergence* 2015, https://www.cio.com/article/2977651/predictive-analytics/why-industrial-iot-platform-is-best-hope-for-it-and-ot-convergence.html [dostęp: 08 VIII 2017]

[16] Standard opracowany w latach 90. XX wieku przez ISO (Międzynarodową Organizację Normalizacyjną) oraz ITU-T (Sektor Normalizacji i Telekomunikacji)

[17] Gralewicz G., Owczarek G. *An inventory of selected electronic, textronic, mechatronic and ICT-based solutions for safety-related applications in smart working environments*" . Materiał oprac. w CIOP-PIB https://www.ciop.pl/CIOPPortalWAR/file/75456/An_inventory_of_selected_ITC_solutions_CIOP-PIB_2015.pdf [dostęp: 08 VIII 2017]

[18] Na podstawie informacji o projekcie *iProtect – Intelligent PPE system for personnel in high risk and complex environments*

[19] Stempień Z., Kozicki M., Pawlak R., Korzeniewska E., Owczarek G., Pościk A., Sajna D. *Ammonia gas sensors ink-jet printed on textile substrates*, Proceedings of 15th IEEE Sensors Conference, 03.11.2016

[20] Mitnick K. *The Art of Invisibility. The World's Most Famous Hacker Teaches ou How to Be Safe in the Age of Big Brother and Big Data.* Hachette Book Group 2017

[21] https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot/at_download/fullReport [dostęp: 19 V 2018]

[22] Bejtlich R. *The Practice of Network Security Monitoring. Understanding Incident Detection and Response 1st Edition*". No Starch Press, 2013

Publikacja opracowana na podstawie wyników IV etapu programu wieloletniego „Poprawa bezpieczeństwa i warunków pracy", finansowanego w latach 2017-2019 w zakresie zadań służb państwowych przez Ministerstwo Rodziny Pracy i Polityki Społecznej. Koordynator programu: Centralny Instytut Ochrony Pracy – Państwowy Instytut Badawczy.