Bezpieczeństwo informacji

w nowoczesnych zakładach produkcyjnych

Automatyzacja odważnie wkracza w produkcyjną codzienność. Staje się nieodzowną normą, oczekiwaną przez wszystkich i sugerowaną przez specjalistów. Nie jest już obecna jedynie w najnowocześniejszych zakładach, np. w branży automotive, lecz także w przemyśle spożywczym, elektronicznym, wydobywczym i wielu, wielu innych. Dzięki stałemu monitoringowi wydarzeń produkcyjnych i procesów możliwe jest przewidywanie i zapobieganie usterkom, wdrażanie strategii predictive maintenance w utrzymaniu ruchu, optymalizowanie zużycia zasobów, efektywne sterowanie czynnościami pozostającymi w korelacji czy zwiększenie bezpieczeństwa pracowników.

Agnieszka Hyla

Aby jednak optymalizacja dzięki automatyzacji miała rację bytu, konieczne jest przekazywanie wszystkich istotnych informacji poprzez sieci komunikacyjne tak, aby w sposób ciągły docierały do konkretnych odbiorników, a także były przechowywane w odpowiednich serwerach, zapewniających ich bezpieczny zapis w celu umożliwienia przeprowadzania analiz danych historycznych i symulacji predykcyjnych.

Bezpieczeństwo infrastruktury

Przemysłowa infrastruktura komunikacyjna musi być zabezpieczona przed różnymi rodzajami ingerencji. Pierwszy z nich stanowią zakłócenia. W najbardziej zaawansowanych zakładach produkcyjnych, w których automatyzacja procesu i komunikacja urządzeń stanowi kluczowy element wartości biznesowej, wykorzystuje się zazwyczaj sieci Profinet. Oferują one lepsze parametry, takie jak szybkość przekazu, rozmiar ramki czy odporność na zakłócenia właśnie względem starszego typu sieci Profibus. W większości przypadków mimo możliwości przesyłania sygnału radiowego przez Profinet, wykorzystuje się połączenie przemysłowym kablem ethernetowym. Kabel tego typu jest specjalnie wzmocniony, aby był odporny na potencjalne zakłócenia. Dobrym przykładem może być tutaj proces zgrzewania, który generuje tak silne pole elektromagnetyczne, że drobniejsze elementy są wręcz poruszane pod wpływem obecności wytwarzanego przez maszynę pola. W związku z tym wszystkie urządzenia wykorzystywane w strefie pracy zgrzewarek muszą mieć odpowiednio wysoką klasę odporności na zakłócenia.

Eliminacja trudnych warunków

Przesył danych może jednak być zagrożony także przez trudne warunki panujące w halach produkcyjnych. Tutaj bardzo wiele zależy od branży. Automotive to szczególny ekosystem – jest tu tak wiele współgrających ze sobą urządzeń, a koszt nieplanowanego przestoju tak wysoki, że czystość produkcji stanowi jeden z istotnych elementów utrzymania ruchu. Wszystko po to, by nie zaburzać pracy urządzeń i z łatwością kontrolować procesy. Nie każda branża może się jednak pochwalić sterylnymi strefami wytwórczymi. Zupełnie inne warunki panują np. w przemyśle wydobywczym czy przetwarzania rud metali. Chemikalia, odłamki, pył, muł, ogromne kontenery i pojemniki na pozyskany materiał. Wszechobecny metaliczny zapach, kurz, oleje i smary. Wszystko

to ma wpływ na to, jakie sieci powinny być wykorzystywane do komunikacji maszyn, a także na ile będą skuteczne. Dodatkową przeszkodą może być wysoka wilgotność czy skrajna temperatura, zarówno wysoka jak i niska. W zakładach tego typu zazwyczaj dominują protokoły takie jak Modbus czy Profibus. To, jakiego producenta protokół jest wykorzystywany zazwyczaj zależy od wynegocjowanych warunków współpracy lub parametrów wyróżniających poszczególne sieci. Połączenia kablem są tutaj jednak preferowane ze względu na większą niezawodność działania w trudnych warunkach. Zapewnienie sprawnej komunikacji układu jest bowiem konieczne. Nie można dopuścić do sytuacji, w której informacje nie są dostarczane, zapisywane lub też dochodzi do zatrzymań pracy wskutek uszkodzenia sieci lub układu sterowania. Koszty nieplanowanego przestoju prawie zawsze przewyższają koszty przemyślanego utrzymania ruchu.

Fot. EMT-Systems

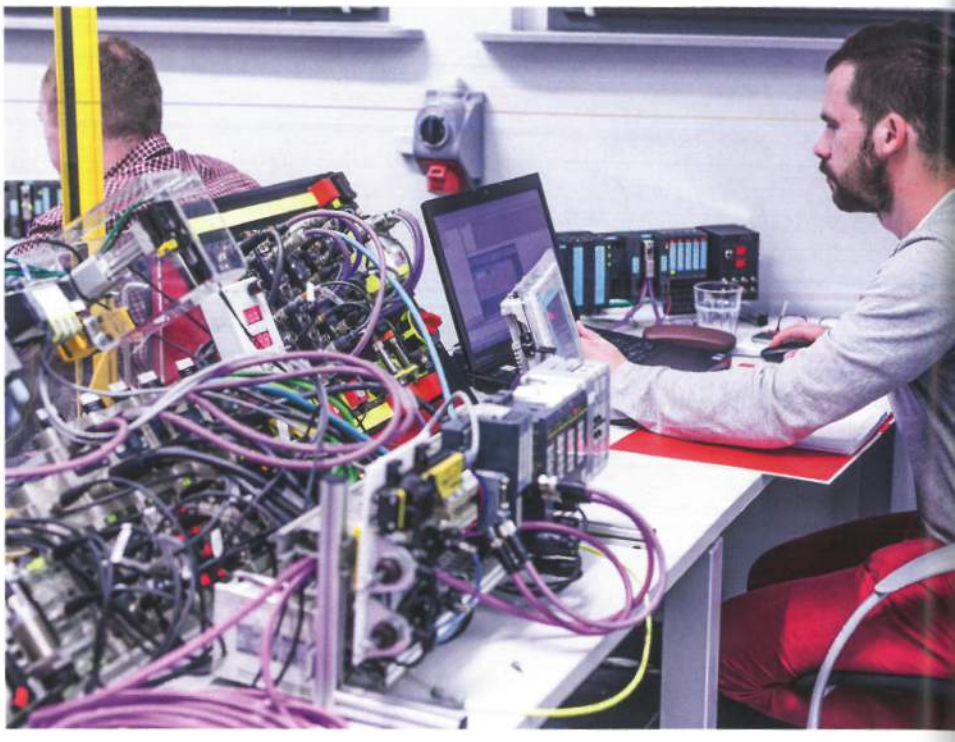
Ataki hakerów

Zakłócenia i trudne warunki pracy to jednak nie jedyne czynniki wpływające na bezpieczeństwo przesyłu informacji w produkcji. Poważne zagrożenie stanowią ataki hakerów i potencjalne wycieki informacji, a w tym przypadku istotnego know-how danej firmy, na zewnątrz. Wiedza i wypracowane przez lata funkcjonowania metody działania to najcenniejszy kapitał firmy. Wynika z długotrwałej współpracy wielu specjalistów różnych dziedzin. Z wykonania setek, a nawet tysięcy iteracji danego procesu, po to by poprawić go o kilka procent. Wypracowywanie dobrych efektów po raz pierwszy jest znacznie droższe od powielania już istniejącego rozwiązania. Dlatego know-how zazwyczaj jest bardzo szanowane i skrzętnie chronione przed kradzieżą. Niestety, w zakładach produkcyjnych coraz częściej dochodzi do wycieków informacji na zewnątrz [1]. Przez to, że coraz częściej do zamkniętych sieci komunikacyjnych w firmach niechcący lub umyślnie podłącza się sieć internetową, złodzieje mają możliwość dostania się do newralgicznych danych, pobrania ich i sprzedaży konkurencji lub na czarnym rynku. Dużo gorszą ewentualnością jest zablokowanie linii produkcyjnej dla okupu. W takiej sytuacji każda godzina postoju to w przypadkach automotive nawet dziesiątki tysięcy euro, czasami setki w zależności od wytwarzanego modelu. Firmy będące w takiej sytuacji zazwyczaj jak najszybciej płacą okup, by tylko uwolnić produkcję. Niestety, przystając na warunki internetowych porywaczy często narażają się na podobne ataki w przyszłości lub niespełnienie żądań mimo dokonania opłaty [2].

Zasady pracownicze

Bezpieczeństwo informacji to jednak także odpowiednie zasady panujące wśród pracowników. Niestety, to ludzie najczęściej powodują, że sieć przemysłowa jest zagrożona. Na przykład przez nieświadome poddawanie

jej oddziaływaniu sieci zewnętrznych. W przypadku, kiedy pracuje się w hali produkcyjnej z zamkniętą siecią komunikacyjną przenoszącą informacje zarówno po kablach jak i radiowo, łączenie się jednostek komputerowych wchodzących w jej skład z Internetem prawie zawsze jest zabronienie. Stąd pracując na komputerze przemysłowym nie można nań udostępnić Internetu, w sposób bezpośredni zagraża to bowiem sieci i całej produkcji. Wiele firm ogranicza ponadto dostęp poszczególnych pracowników do wiedzy i urządzeń. Wszystko po to, by minimalizować zagrożenie wynikające z nadużywania dostępów oraz powierzania zbyt dużej ilości informacji newralgicznych dużym grupom ludzi. Stąd w halach produkcyjnych spotyka się przepustki jednodniowe, tygodniowe lub miesięczne. Jeśli pracownik posiada prywatnego laptopa lub telefon często musi na kamerki naklejać specjalne ograniczniki, których oderwanie jest wyraźnie rozpoznawalne. Cały wnoszony przez pracownika sprzęt jest często spisywany na specjalnej liście inwentaryzacyjnej – każde narzędzie, urządzenie, komunikator. W bardziej uważnych firmach w zakładzie pojawiają się co jakiś czas zespoły kontrolne, które weryfikują czy posiadany sprzęt znajduje się na odpowiedniej liście i czy został sprawdzony. Także dostęp do różnych pomieszczeń jest ograniczany. Zazwyczaj pracownik pracujący np. na linii montażu drzwi ciężarówki ma dostęp wyłącznie do tej hali oraz ewentualnie do pomieszczeń socjalnych lub tych, które musi minąć, by dostać się do swojego miejsca pracy. Ogranicza to zbędną migrację pracowników, oszczędza czas, a dodatkowo minimalizuje dostęp do szerszego know-how. Wszystko jednak zależy od hierarchii w firmie i poziomu odpowiedzialności pracy danego pracownika. Spawacze, których zazwyczaj w firmach produkcyjnych brakuje, mają wysoki poziom dostępu, ponieważ pracują w wielu działach. Tak samo jest w przypadku kierowników, pracowników wyższego szczebla. Oni otrzymują wyższy poziom przepustek, ponieważ są odpowiedzialni za przebieg większości kluczowych procesów. W taki sam sposób



pod tym względem traktowani są pracownicy wewnętrzni firm jak i kontraktorzy zewnętrzni, nie ma tutaj większej różnicy. Tylko pracownicy wyższego szczebla mają dostęp do newralgicznej wiedzy o procesach produkcyjnych, szczególnie tych, które stanowią przewagę konkurencyjną firmy na rynku.

Pracownicy rozpoczynając pracę w danej firmie otrzymują wszystkie niezbędne do jej wykonywania informacje – wiedzę, know-how, dokładne opisy procesów, metod, parametrów i technologii wykorzystywanych na danym stanowisku. Można się z tymi informacjami zapoznać, wykorzystuje się je bowiem w codziennej pracy. W teorii nie można ich przekazywać osobom postronnym, jednak tylko niektóre firmy zadają sobie trud, żeby poinformować pracowników o tym, które informacje stanowią krytyczne know-how, a które można rozpowszechniać np. podczas konsultacji z innymi specjalistami. Może więc dojść do nieświadomego przekazania tajemnicy firmy, co może mieć poważne konsekwencje. Ponadto nie ma *de facto* sprawdzonego sposobu na ograniczanie wyciekania informacji firmowych generowanego właśnie przez pracowników, zazwyczaj tych z jakiegoś powodu niezadowolonych. Warto więc dbać o morale pracowników bez względu na miejsce w firmowej hierarchii i poświęcać czas na edukowanie oraz informowanie o zagrożeniach związanych z nieświadomym narażeniem przemysłowej sieci na atak, a także ograniczać wynoszenie danych z firmy przez przemyślane udzielanie dostępów i przepustek.

Podsumowanie

Zapewnianie bezpieczeństwa informacji w dzisiejszych czasach jest dla firm produkcyjnych zagadnieniem ważnym i trudnym. Źle zaplanowane i wdrożone może spowodować ogromne, nieplanowane koszty. Wprowadzając unowocześnienia w już istniejących systemach warto więc wziąć pod uwagę aspekt bezpieczeństwa, by uniknąć nieodwracalnych strat, nie tylko finansowych. ■

Agnieszka Hyla
EMT-Systems
Centrum Szkoleń Inżynierskich

Źródła:

[1] Zmasowany atak hakerów. Premier zwołała sztab kryzysowy, Newsweek, http://www.newsweek.pl/polska/atak-hakerow-zaatakowane-polskie-firmy,artykuly,412431,1.html, dostęp z dnia 02.01.2018

[2] Wielki atak hakerów. Świat się zbroi, a polskie firmy liczą na szczęście, money.pl, https://www.money.pl/gospodarka/ngospodarka/ebiznes/artykul/atak-hakerow-cyberbezpieczenstwo-wlamanie-do,88,0,2318424.html, dostęp z dnia 02.10.2018