aut. Tomasz Fastyn 06.09.2016

DIGITALIZACJA INFRASTRUKTURY PRZEMYSŁOWEJ WYMUSZA ZMIANY W PODEJŚCIU DO CYBERBEZPIECZEŃSTWA

Jedna z międzynarodowych firm ARC Group, zajmująca się drukowanie 3D opublikowała raport dotyczący digitalizacji procesów produkcji i wiążących się z tym problemów cyberbezpieczeństwa. Działy zajmujące się cyberbezpieczeństwm przemysłu sprostały oczekiwaniom oraz są odpowiednio przygotowane na cyberataki.

Według raportu *How Digitalization is Changing the Face of Cyber Security* wiele rzeczy zmieniło się na dużo lepsze, jednak nie było by to możliwe bez trzech podstawowych zasad, którymi aktualnie kierują się niemal wszystkie firmy. Chodzi o integracje systemów, bezpieczeństwo sieci oraz bezpieczeństwo samych fabryk. Jak zaznacza autor raportu to dobry ruch w odpowiednią stronę, większość firm odpowiednio przygotowało się na zagrożenia pochodzące z sieci i implementuję dobre rozwiązania z zakresu cyberbezpieczeństwa.

Problem z obecnymi atakami nie tylko w infrastrukturze przemysłowej, ale także w firmach zajmujących się infrastrukturą krytyczną czy energetyczną pojawił się dopiero z czasem. Wcześniej jak zauważa twórca raportu, wszystkie systemy działały na zasadach analogowych, więc zdalny dostęp do nich był po prostu nie możliwy. Zmieniło się to przy wprowadzaniu możliwości zdalnego oraz cyfrowego zarządzania produkcją czy przesyłaniem energii np. na terenie kraju.

Pozwalało to także na większą automatyzację procesów, co prowadziło do polepszenia wydajności. Jednak jak przedstawia raport przez ostatnie kilka lat nieodpowiednio pochylano się nad kwestią samego cyberbezpieczeństwa systemów informatycznych czy kwestii związanych z ochroną samych pracowników, którzy mogą stać się mimowolnie, koniem trojańskim w rękach hakerów. Np. przynosząc ze sobą do pracy zainfekowane urządzenie.

Problem miał polegać na kompletnie różnych priorytetach w różnych firmach. Firmy przemysłowe swoją uwagę skupiały głównie na czasie dostępności, długości działania oraz awaryjności samych systemów informatycznych. Podczas kiedy inne firmy, zajmujące się cyberbezpieczeństwem sieci użytkowej, swoje priorytety skupiały na bezpieczeństwie informacyjnym czy integralności systemów.

Stąd też przeniesienie bezpiecznych praktyk z jednej branży do drugiej, bez określenia najważniejszych elementów sieci jest zdaniem ARC bezsensowne i kompletnie błędne, jeżeli chodzi o zabezpieczenie przemysłu. To miało właśnie dziać się w początkowych latach digitalizacji systemów zarządzania produkcją i takie niedopasowane odpowiednio do innej branży rozwiązania miały stosować firmy informatyczne. Stąd też miały pojawiać się późniejsze problemy bezpieczeństwa całego sektora, z prostego nie zrozumienia potrzeb jaki on ma obecnie.

Jednocześnie raport skupia się na przyszłych oraz obecnych problemach związanych z rozwojem

technologii – chmurą obliczeniową oraz Internetem Rzeczy. Zauważa, że rozwój oraz implementacja tych dwóch elementów spowoduję jeszcze większe narażenie całej linii produkcyjnej czy elektrowni atomowej na możliwość dokonania cyberataku, dlatego też należy potraktować samą kwestię cyberbezpieczeństwa bardzo poważnie. Nie chodzi bowiem w tym przypadku o chwilowe zatrzymanie produkcji, ale możliwość skażenie całego regionu poprzez związki chemiczne czy promieniowanie. Ważna jest w tym przypadku także odpowiednia wymiana informacji pomiędzy firmami, tak aby czerpać wiedzę z dobrych praktyk czy sytuacji kryzysowych.

Czytaj też: Chiński szpieg w elektrowni atomowej