Informacje ogólne

Pilz GmbH & Co. KG
Felix-Wankel-Straße 2
73760 Ostfildern, Niemcy
Deutschland/Niemcy
www.pilz.com

16 maja 2024 r.

Ochrona produktów, maszyn i zakładu

Ochrona i bezpieczeństwo przemysłowe – wszystko od jednego dostawcy

Ostfildern, 16 maja 2024 r. – **Incydenty związane z naruszeniem bezpieczeństwa nie dotyczą już tylko systemów IT, ale w coraz większym stopniu także środowiska produkcyjnego (OT). Natomiast incydenty związane z naruszeniem bezpieczeństwa przemysłowego obejmują nie tylko ukierunkowane ataki, ale także niezamierzone manipulacje. Bezpieczeństwo przemysłowe ma na celu zagwarantowanie ciągłości pracy instalacji i maszyn oraz integralności i poufności danych i procesów produkcji. Jeśli przedsiębiorstwa nie nadzorują swoich danych, zagrożone jest bezpieczeństwo zarówno samego przedsiębiorstwa, jak i jego pracowników.**

Unia Europejska zareagowała na rosnący poziom zagrożeń wydając **Dyrektywę w sprawie bezpieczeństwa sieci i informacji NIS 2,** która nakłada na przedsiębiorstwa wymóg pełnego wdrożenia systemu zarządzania bezpieczeństwem informacji.

Nowe Rozporządzenie UE w sprawie maszyn 2023/1230 przewiduje obecnie ochronę instalacji i maszyn przed naruszeniem integralności oraz wymaga stosowania środków bezpieczeństwa w odniesieniu do tych części maszyny, które mają wpływ na bezpieczeństwo funkcjonalne.

Ustawa **Cyber Resilience Act (CRA)** wymaga zastosowania środków bezpieczeństwa w odniesieniu do produktów zawierających elementy cyfrowe, do których należą sterowniki, systemy we/wy i inne komponenty stosowane w maszynach.

Na każdym etapie konstruktorzy i operatorzy maszyn stoją przed przeróżnymi wyzwaniami i muszą uwzględniać wymagania prawne wielu różnych przepisów.

Niezależnie od tego, czy ustawodawca nakłada obowiązek zapewnienia bezpieczeństwa przemysłowego, istnieje wiele powodów, dla których warto się tym zagadnieniem zapoznać wcześniej. Wiele procedur i czynników związanych z działaniem maszyn sprzyja manipulacji. Dlatego należy je pilnie zweryfikować i zmodyfikować. Długi okres eksploatacji maszyn często prowadzi do sytuacji, w których systemy przestają spełniać aktualne standardy bezpieczeństwa. Mogą one również posiadać luki w zabezpieczeniach, których nie można już usunąć, ponieważ producent zaprzestał dostarczania aktualizacji zabezpieczeń. Nierzadko ochrona przed złośliwym oprogramowaniem nie może zostać wdrożona na urządzeniach końcowych, gdyż są one zbyt przestarzałe. Cierpią na tym ich parametry użytkowe, co może prowadzić do przestojów w produkcji.

Kompleksowy pakiet usług firmy Pilz

Ostatecznym celem każdego przedsiębiorstwa jest ochrona działalności biznesowej, ale wiąże się to z wieloma wyzwaniami. Począwszy od ustalenia obowiązujących wymogów prawnych oraz wykrywania i korygowania słabych punktów w systemach, a skończywszy na podnoszeniu świadomości i szkoleniu pracowników oraz późniejszym egzekwowaniu wymaganych działań. Ponieważ bezpieczeństwo jest celem, którego założenia ciągle się zmieniają, konieczna jest również regularna kontrola stanu bezpieczeństwa przemysłowego maszyn.

Firma Pilz przygotowała dedykowany pakiet usług dla konstruktorów i użytkowników maszyn na całym świecie, obejmujący wszystkie

aspekty ochrony ludzi i maszyn. W jego ramach dostępne są nie tylko podstawowe informacje, przewodniki i szkolenia, ale też nowa usługa Industrial Security Consulting Service (ISCS), w ramach której realizowane są projekty.

„CESA – Certified Expert for Security in Automation” to oferowane przez firmę Pilz dodatkowe dwudniowe szkolenie eksperckie, w trakcie którego uczestnicy zdobywają wiedzę na temat bezpieczeństwa zgodnie z obowiązującymi normami. Szkolenie uwzględnia praktyczne działania ukierunkowane na ograniczenie ryzyka, takie jak kontrola dostępu, środki techniczne zwiększające bezpieczeństwo sieci oraz środki organizacyjne mające na celu uniknięcie zagrożeń dla bezpieczeństwa. Po jego zaliczeniu uczestnicy otrzymają uznawany na całym świecie certyfikat TÜV NORD „CESA – Certified Expert for Security in Automation”.

W ramach usługi Industrial Security Consulting Service (ISCS) firma Pilz poszerza zakres kontroli bezpieczeństwa maszyn, stawiając na kompleksowe podejście do ochrony i bezpieczeństwa. ISCS bazuje na sprawdzonej metodologii usług w zakresie bezpieczeństwa funkcjonalnego maszyn oraz w oparciu o wymogi serii norm IEC 62443. Skorzystanie z usługi umożliwia przedsiębiorstwom uzyskanie wysokiego poziomu bezpieczeństwa przemysłowego oraz spełnienie aktualnych wymagań prawnych.

ISCS gwarancją wzrostu bezpieczeństwa przemysłowego

Usługa ISCS obejmuje cztery moduły: Analiza wymagań w zakresie ochrony, ocena ryzyka w ramach bezpieczeństwa przemysłowego, koncepcja bezpieczeństwa przemysłowego i weryfikacja systemu bezpieczeństwa przemysłowego.

W ramach analizy wymagań w obszarze ochrony ustalany jest zakres oraz cele ochrony poszczególnych „aktywów” wchodzących w skład instalacji. Krok drugi to ocena ryzyka, podczas której rozważane są wszystkie zagrożenia – wraz z prawdopodobieństwem ich wystąpienia – dla każdego elementu w całym cyklu życia systemu. Następnie eksperci firmy Pilz spotykają się z klientem, aby omówić rozwiązania mające na celu eliminację wykrytych luk w zabezpieczeniach oraz potencjalnych zagrożeń.

W kroku trzecim przygotowywana jest koncepcja bezpieczeństwa przemysłowego obejmującą strategie i środki zapobiegania atakom oraz przypadkom niewłaściwego użycia i manipulacji. Ponadto tworzone są wytyczne wymagane z punktu widzenia zapewnienia ciągłej bezpiecznej pracy lub integralności systemu. W ostatnim kroku prowadzona jest weryfikacja systemu bezpieczeństwa przemysłowego mająca na celu kontrolę skuteczności wdrożonych środków zaradczych.

Zapewnienie ciągłości pracy maszyn

Usługa Industrial Security Consulting Service pomaga łagodzić skutki cyberataków oraz zapobiegać im. Pozwala również na zmniejszenie liczby wywołanych w sposób niezamierzony incydentów związanych z bezpieczeństwem. To z kolei zwiększa gwarancję ciągłości pracy maszyn, a tym samym przynosi firmie oszczędności i pozwala utrzymać efektywność ekonomiczną.

Jednak przede wszystkim usługa ISCS skupia się na zapewnieniu odpowiednich środków bezpieczeństwa w celu ochrony osób pracujacych przy maszynie. Incydenty związane z bezpieczeństwem mogą bowiem zakłócić działanie środków bezpieczeństwa. Na przykład: kurtyna optyczna stanowi gwarancję, że maszyna zatrzyma się w bezpieczny sposób, gdy operator wejdzie do strefy

niebezpiecznej. W przypadku, gdy atak zakłóci działanie określonego sterownika lub mechanizmu, może to spowodować utratę funkcji ochronnej kurtyny optycznej. Odpowiednia ochron zapewnia bezpieczeństwo!

Konstruktorzy i użytkownicy maszyn otrzymują od firmy Pilz zestaw zaleceń, uwzględniających wszystkie aspekty ochrony ludzi i maszyn.

Dlatego też w ramach uruchamiania maszyny uzasadnione jest łączne rozważenie zagadnień ochrony i bezpieczeństwa. Nie ma bowiem ochrony bez bezpieczeństwa, a brak ochrony stanowi zagrożenie dla ludzi!

Jasna kontrola nad zakresem dozwolonych czynności

Bezpieczeństwo maszyn i operatorów zależy od zapewnienia odpowiedniej kontroli dostępu do maszyn i instalacji – zarówno fizycznej, jak i sieciowej. Punkty dostępu należy zabezpieczyć przed niepowołanymi osobami, tak aby nikt nie mógł przebywać w strefie zagrożenia podczas pracy maszyny. Jeśli w takiej strefie znajduje się upoważniony operator, który prowadzi prace konserwacyjne, należy koniecznie zadbać o to, aby nikt inny nie mógł uruchomić maszyny w tym samym czasie. W przeciwnym razie nawet wykonywane w dobrej wierze czynności obsługowe lub konserwacyjne – czy to lokalnie, czy za pośrednictwem sieci – mogą mieć fatalne konsekwencje.

Ważną kwestią są odpowiednio przygotowane zasady identyfikacji i zarządzania dostępem do maszyny (I.A.M.) oraz przejrzyste reguły przyznawania uprawnień do wykonywania danych czynności w ramach zdefiniowanych obowiązków. Należą do nich środki i specyfikacje organizacyjne, a także odpowiednie funkcje bezpieczeństwa i ochrony. System kontroli uprawnień dostępu

PITreader firmy Pilz to istotny składnik, który pozwala zagwarantować ochronę pracowników, ochronę przed odpowiedzialnością prawną, maksymalną produktywność oraz ochronę danych.

System wyboru trybu pracy i kontroli uprawnień dostępu PITmode fusion firmy Pilz umożliwia realizację funkcjonalnie bezpiecznego wyboru trybu pracy oraz kontrolowanie uprawnień dostępu do instalacji i maszyn. Każdy operator otrzymuje transponder z kodem RFID, który zapewnia dostęp do funkcji maszyny zgodnie z obowiązkami i kwalifikacjami. Dzięki temu instalacja może być obsługiwana wyłącznie przez upoważniony personel w określonych trybach pracy. Zapewnia to wysoki poziom ochrony przed niezamierzonymi działaniami i manipulacjami.

Wyposażenie systemu wyboru trybu pracy i kontroli uprawnień dostępu w modułowy system ryglowania pozwala uzyskać spójną koncepcję dostępu do maszyny – z punktu widzenia ochrony i bezpieczeństwa.

Najlepsze zabezpieczenie za pomocą bramki bezpieczeństwa staje się bezwartościowe, jeżeli know-how przedsiębiorstwa i dane operacyjne nie są wystarczająco zabezpieczone przed nieuprawnionym dostępem i manipulacją, gdy osoba postronna może wniknąć do sieci sterowania lub dokonać ingerencji w system sterowania.

Przemysłowy firewall chroni przed dostępem z zewnątrz

Zadaniem modułu SecurityBridge firmy Pilz jest zagwarantowanie ochrony przed zewnętrznym dostępem do sieci automatyki. Monitoruje on przepływ danych pomiędzy komputerem a sterownikiem, zmniejszając w ten sposób przestrzeń narażoną na

ataki hakerskie i manipulacje. Chroni przed manipulacją sterowniki nie tylko firmy Pilz, ale także innych producentów.

Tylko kompleksowe podejście do ochrony i bezpieczeństwa pozwala odpowiednio zabezpieczyć ludzi i maszyny. Decyzja o tym, czy i w jakim stopniu zająć się kwestiami bezpieczeństwa, nie leży już wyłącznie w gestii firmy, a stanowi obecnie wymóg prawny. W branży przemysłowej, bezpieczeństwo przemysłowe nie jest wyłącznie domeną działu IT, lecz stanowi integralny element projektowania i budowy maszyn. Wdrożenie dodatkowych elementów bezpieczeństwa w ramach doposażenia jest skomplikowane i zwykle oznacza pogorszenie łatwości obsługi, funkcjonalności i produktywności.

((Liczba znaków: 10 173))

((Ramka:))

Przegląd prawodawstwa UE dotyczącego bezpieczeństwa przemysłowego

Unia Europejska podjęła stanowcze działania legislacyjne w odpowiedzi na wzrost poziomu zagrożeń cyberatakami. Obecnie w Europie obowiązywać będą najsurowsze na świecie wymagania. Jednak ze względu na obowiązujące umowy z innymi krajami tam też zostaną wprowadzone podobne przepisy. Należy zatem spodziewać się globalnej harmonizacji wymogów dotyczących bezpieczeństwa przemysłowego.

NIS 2: Więcej obowiązków przedsiębiorstw

NIS (Network and Information Security) to dyrektywa Unii Europejskiej mająca na celu wzmocnienie cyberbezpieczeństwa. Obowiązuje od 2016 r. i do tej pory dotyczyła dostawców infrastruktury krytycznej, w tym energii, ruchu, banków i finansów, zdrowia, zaopatrzenia w wodę pitną i jej dystrybucji oraz infrastruktury cyfrowej. Dostawcy w tych branżach musieli wdrożyć „odpowiednie zabezpieczenia" i zgłaszać wszelkie poważne incydenty związane z cyberbezpieczeństwem. W przyszłości nowa Dyrektywa dotycząca bezpieczeństwa sieci i informacji UE 2022/2555 (NIS 2) zobowiąże znacznie więcej podmiotów do podjęcia środków zarządzania ryzykiem w celu zapewnienia odpowiedniego poziomu bezpieczeństwa. Rozszerza ona zasięg przepisów na inne sektory, włączając na przykład branżę produkcyjną, w tym projektantów i producentów sprzętu elektrycznego.

Wymagania obejmują przygotowanie analizy ryzyka i koncepcji bezpieczeństwa dla systemów informatycznych, ochronę łańcucha dostaw oraz zapewnienie bezpieczeństwa personelu. Obok obowiązkowych szkoleń dla kadry kierowniczej wymagane jest również wdrożenie koncepcji kontroli uprawnień dostępu do instalacji.

Dyrektywa została przyjęta przez Parlament Europejski i Radę UE pod koniec 2022 r. Podobnie jak wszystkie inne dyrektywy unijne Dyrektywa NIS 2 nie jest od razu wiążąca, ale musi zostać włączona do prawa krajowego w poszczególnych państwach członkowskich UE. Państwa członkowskie UE mają czas do 18.10.2024 r. na transpozycję dyrektywy do prawa krajowego. Przedsiębiorstwa powinny jak najszybciej przygotować się na wejście w życie Dyrektywy NIS 2 i przeprowadzić kompleksową ocenę własnego bezpieczeństwa. Obejmuje to na przykład opracowanie systemu

zarządzania bezpieczeństwem informacji (ISMS) zgodnie z normą ISO 27001.

Zgodnie z treścią Dyrektywy NIS 2 nowym wymogom będą musieli w przyszłości sprostać także producenci instalacji energetycznych (np. turbin wiatrowych). Z kolei producenci turbin wiatrowych potrzebują komponentów automatyki, sterowników i czujników. Od określonej wielkości przedsiębiorstwa producenci podzespołów elektrycznych również podlegają wymogom dyrektywy NIS 2. A ponieważ zapisy Dyrektywy NIS 2 uwzględniają także dostawców, firmy takie jak Pilz muszą również zatroszczyć się o bezpieczne łańcuchy dostaw i postawić wymagania swoim dostawcom. Jak widać, wymogi dyrektywy NIS 2 rozciągają się na cały łańcuch dostaw.

Nowe Rozporządzenie UE w sprawie maszyn

Dyrektywa maszynowa 2006/42/WE odgrywa istotną rolę w kwestii bezpieczeństwa funkcjonalnego maszyn.

Każda maszyna sprzedawana w Europie musi przejść odpowiednią procedurę oceny zgodności zakończoną nadaniem znaku CE.

Opublikowane w czerwcu 2023 r. Rozporządzenie w sprawie maszyn uwzględnia aktualny stan rozwoju techniki. Ponieważ przepisy mają formę rozporządzenia, nie muszą zostać przetransponowane do prawa krajowego. Producenci maszyn mają czas do 20.01.2027 r. na dostosowanie się do nowych wymagań.

Rozporządzenie w sprawie maszyn zastępuje istniejącą dyrektywę maszynową i wprowadza dodatkowy wymóg dotyczący zapewnienia cyberbezpieczeństwa. Podczas gdy dyrektywa maszynowa dotyczyła jedynie bezpieczeństwa, nowe rozporządzenie uwzględnia cel

ochrony bezpieczeństwa wyrażony w „Zasadniczych wymaganiach w zakresie zdrowia i bezpieczeństwa”, w części „Ochrona przed naruszeniem integralności”: Funkcje ochrony maszyny nie mogą ulec pogorszeniu w wyniku naruszenia integralności – czy to zamierzonego, czy przypadkowego.

Nowa droga do oznakowania maszyn znakiem CE stwarza wiele problemów dla konstruktorów i operatorów maszyn, którzy muszą zrewidować istniejące koncepcje ochrony i bezpieczeństwa.

Ustawa Cyber Resilience Act: bezpieczeństwo w całym cyklu życia produktu

Oprócz zbadania stanu przedsiębiorstwa i maszyn bezwzględnie konieczne jest również zastosowanie środków ochrony bezpośrednio w urządzeniach (takich jak sterowniki). We wrześniu 2022 r. Komisja Europejska przedstawiła projekt rozporządzenia, którego celem jest zwiększenie cyberbezpieczeństwa produktów. Przepisy ustawy Cyber Resilience Act (CRA) są skierowane do producentów komponentów zawierających składniki cyfrowe (sprzęt i oprogramowanie), które potrafią komunikować się z innymi produktami. Dotyczy to zarówno produktów z segmentu B2C, takich jak smartfony czy odkurzacze automatyczne, jak i produktów z segmentu B2B, takich jak sterowniki i czujniki, a także produktów programistycznych, takich jak systemy operacyjne, czy samych maszyn.

Rzeczywisty wpływ przepisów CRA zależy ostatecznie od ustalonych kryteriów klasyfikacji produktów. Zgodnie z wymaganiami ustawy CRA na rynek mogą trafiać wyłącznie produkty gwarantujące odpowiedni poziom cyberbezpieczeństwa – w całym cyklu swojego życia. Bezpieczeństwo zaczyna się więc już na etapie

opracowywania produktu. Z tego powodu w ostatnich latach firma Pilz dostosowała swoje procesy rozwoju do wymogów normy IEC 62443-4-1 „Bezpieczeństwo systemów automatyki przemysłowej i sterowania – Część 4-1: Wymagania cyklu rozwoju dotyczące tworzenia bezpiecznego produktu” oraz opracowała moduł SecurityBridge, który pełni rolę przemysłowego firewalla.

((Liczba znaków: 5826))

Rysunki

Rys. 1:

Grafik_aus_Prospekt_Schulungen_mit_Pilz_3c_en_ppt

Bezpieczeństwo i ochrona od jednego dostawcy: firma Pilz oferuje kompleksowy pakiet rozwiązań obejmujących usługi i produkty z zakresu bezpieczeństwa przemysłowego maszyn. (Zdjęcie: © Pilz GmbH & Co. KG)

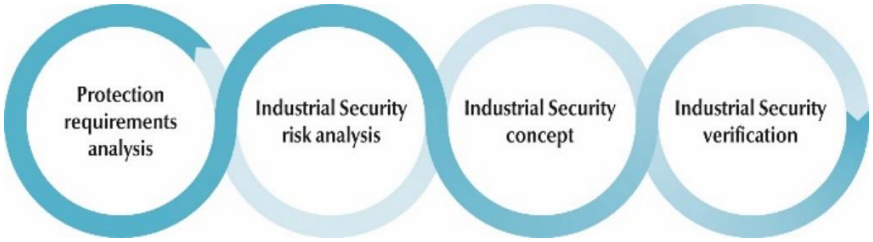
Rys. 2:

F_Services_ISCS_two_men_tablet_in_discussion_get1150297892_cold1

Firma Pilz wprowadza do oferty nową usługę Industrial Security Consulting Service, aby pomagać firmom dbać o bezpieczeństwo instalacji i maszyn. (Zdjęcie: © Westend61/[westend61] z zasobu Getty Images, © Pilz GmbH & Co. KG)

Rys. 3:

G_Cycle_Industrial_Security_en



Usługa Industrial Security Consulting Service firmy Pilz obejmuje cztery moduły: Analiza wymagań w zakresie ochrony, ocena ryzyka w ramach bezpieczeństwa przemysłowego, koncepcja bezpieczeństwa przemysłowego i weryfikacja systemu bezpieczeństwa przemysłowego. (Zdjęcie: © Pilz GmbH & Co. KG)

Rys. 4:

F_Press_IAM_Man_using_PITreader_Key_Get1169337234_Get1169337153_cold1

Kompleksowe zasady identyfikacji i zarządzania dostępem nadzorują dostęp do instalacji, zapewniając w ten sposób integralność funkcji i środków bezpieczeństwa – w tym ochrony i bezpieczeństwa przemysłowego. (Zdjęcie: © Westend61/[westend61] z zasobu Getty Images, © Pilz GmbH & Co. KG)

Rys. 5:

F_security_robot_man_virtual_world_Fot208731449_cold1_2019_06

Bezpieczeństwo przemysłowe to ochrona zakładów przemysłowych przed zamierzonymi lub niezamierzonymi zagrożeniami i awariami. Jego celem jest zagwarantowanie ciągłości pracy instalacji i maszyny oraz integralności i poufności danych i procesów. (Zdjęcie: © ipopba/Fotolia.com; © Pilz GmbH & Co. KG)

Pilz – The Spirit of Safety

Firma Pilz jest globalnym dostawcą produktów, systemów i usług w dziedzinie technologii automatyzacji. Jako pionier w dziedzinie bezpieczeństwa automatyzacji firma Pilz tworzy rozwiązania zapewniające bezpieczeństwo ludzi, maszyn

i środowiska. Założona w 1948 r. firma rodzinna z Ostfildern zatrudnia obecnie około 2500 osób w 42 oddziałach na całym świecie.

Jako lider technologii przedsiębiorstwo oferuje kompletne rozwiązania automatyzacji dla bezpieczeństwa i ochrony przemysłowej maszyn. Obejmują one technologie czujników, sterowania i napędów – w tym systemy komunikacji, diagnostyki i wizualizacji przemysłowej. Uzupełnieniem oferty są świadczone na całym świecie usługi doradcze, inżynieryjne i szkoleniowe. Rozwiązania firmy Pilz są wykorzystywane w wielu branżach poza inżynierią mechaniczną, na przykład w branży intralogistyki, maszyn pakujących, technologii kolejowej czy robotyki.

www.pilz.com

Firma Pilz w mediach społecznościowych

Na naszych kanałach w mediach społecznościowych udostępniamy podstawowe informacje o firmie i personelu oraz przekazujemy najświeższe aktualności ze świata technologii automatyzacji.

www.pilz.com/facebook
www.pilz.com/X
www.pilz.com/xing
www.pilz.com/youtube
www.pilz.com/linkedin

Kontakt z mediami:

Martin Kurth
Corporate and Technical Press
Tel.: +49 711 3409-158
m.kurth@pilz.de

Sabine Karrer
Prasa korporacyjna i techniczna
Tel.: +49 711 3409-7009
s.skaletz-karrer@pilz.de

Eva Rössle
Prasa techniczna
Tel.: +49 711 3409-7147
e.roessle@pilz.de

Hansjörg Sperling-Wohlgemuth
Zarządzanie konferencjami i prezentacjami
Tel.: +49 711 3409-239
h.sperling@pilz.de