Bezpieczeństwo

PILZ
THE SPIRIT OF SAFETY

Biała księga

Zastrzeżenia prawne

Nasza Biała księga została sporządzona z najwyższą starannością. Zawiera ona informacje o naszej spółce i naszych produktach. Cała jej treść odpowiada aktualnemu stanowi technologii i powstała zgodnie z naszą najlepszą wiedzą. Mimo że uczyniliśmy wszystko, aby uczynić zamieszczone informacje wyczerpującymi, nie odpowiadamy za ich kompletność i dokładność, z wyjątkiem poważnych niedokładności. Należy zauważyć, że użyte stwierdzenia nie są mają mocy prawnej. Prosimy o wszelkie opinie dotyczące niniejszej treści.

Informacje o prawach autorskich

Pilz GmbH & Co. KG
Felix-Wankel-Straße 2
73760 Ostfildern
Niemcy

Szybko i przejrzyście

Dzięki cyfryzacji fabryk systemy w coraz większym stopniu podlegają usieciowieniu. Co powoduje wzrost ryzyka związanego ze szpiegostwem lub manipulowaniem ważnymi danymi. W przeszłości komunikacja w dziedzinie automatyzacji odbywała się głównie za pośrednictwem takich magistrali jak CAN, a także za pośrednictwem protokołów własnych producenta. Aby wyrządzić jakąkolwiek szkodę, atakujący musiałby wejść do hali fabrycznej lub uzyskać dostęp do maszyny za pośrednictwem linii telefonicznej z modemem. Ponieważ modemy te są obecnie w coraz większym stopniu zastępowane przez protokoły Ethernet i IP, ataki mogą być przeprowadzane za pośrednictwem internetu.
Ich motywami mogą być zamiary terrorystyczne, szpiegostwo przemysłowe i sabotaż systemów polegający na wymuszaniu okupów. Próby ataków ułatwia zwiększone wykorzystywanie w automatyzacji oprogramowania typu open-source i podzespołów oprogramowania pochodzących z sektora konsumenckiego, który potencjalnie jest mniej odporny na zagrożenia, z czego atakujący doskonale zdają sobie sprawę. Zatem ochrona w kontekście konieczności zabezpieczenia danych produkcyjnych nabiera coraz większego znaczenia.
Z doświadczenia wiemy, iż komunikat ten nie jest jeszcze w pełni zrozumiały dla wszystkich. Dlatego w niniejszej białej księdze przedstawimy zasadnicze aspekty bezpieczeństwa i rozwiązania, które dowodzą w praktyce swojej zasadności. W rezultacie budowniczy maszyn, projektanci instalacji, technicy instalacyjni i konserwatorzy mogą stwierdzić, jaką rolę odgrywają ich produkty lub usługi w strategiach ochrony danych ich klientów, i na co muszą zwrócić uwagę. Do rozważań włączono ponadto aspekt bezpieczeństwa funkcjonalnego. Ponieważ zarówno ochrona danych, jak i bezpieczeństwo procesów są elementem bezpiecznych procesów produkcyjnych.

Spis treści

1. Ochrona i bezpieczeństwo danych

1.1. Definicja

W przeszłości ochrona i bezpieczeństwo danych odnosiły się niemal wyłącznie do klasycznej technologii IT. Obecnie obszary IT i automatyzacji coraz ściślej ze sobą współpracują. Stopień podłączenia do sieci instalacji produkcyjnych i użytkowania standardowych protokołów, takich jak Ethernet, do fizycznego przekazywania danych wzrastają w coraz większym stopniu. Ponadto unormowane protokoły takie jak OPC UA pozwalają na dostęp do sterowników za pośrednictwem systemów IT, przy czym komunikowanie danych staje się coraz bardziej otwarte.
W automatyzacji termin ochrona oznacza przede wszystkim zabezpieczenia instalacji lub maszyny przed nieuprawnionym dostępem z zewnątrz oraz zabezpieczenia wrażliwych danych przed sfałszowaniem, utratą lub nieuprawnionym dostępem od wewnątrz. Zagrożenia pochodzą z cyberświata, który obejmuje internet, a także całej współczesnej technologii informacyjnej oraz komunikacyjnej. Ochrona rozpoczyna się od ochrony dostępu na wejściu fizycznym do instalacji i rozciąga się na wszystkie aspekty ochrony przed działaniami hakerów. Jednak zdaniem niemieckiego eksperta ds. bezpieczeństwa IT, Ralpha Langnera, nie zawsze szkodę wyrządzają „źli ludzie". Szereg naruszeń bezpieczeństwa odbywa się w sposób niezamierzony, na przykład z powodu błędów obsługi, popełnionych przez nieświadomych pracowników.
Termin bezpieczeństwo oznacza funkcjonalne bezpieczeństwo instalacji w znaczeniu ochrony ludzi i środowiska przed dającymi się przewidzieć zagrożeniami, które mogą stwarzać maszyny. Ryzyko resztkowe, obecne zawsze w większym lub mniejszym stopniu, nie może tutaj przekraczać dopuszczalnych poziomów. Jedną z metod zagwarantowania odpowiedniego poziomu bezpieczeństwa jest stosowanie odpowiednich podzespołów takich jak przekaźniki bezpieczeństwa i czujniki bezpieczeństwa utrzymujące maszynę w bezpiecznym stanie.
Po zatwierdzeniu bezpieczeństwa funkcjonalnego maszyny zgodnie z wymaganiami dyrektywy maszynowej, operatorzy instalacji zazwyczaj nie obawiali się o bezpieczeństwo, o ile w okresie późniejszym nie wprowadzano na maszynie żadnych zmian. Te czasy, niestety, należą już do przeszłości. Z racji zagrożeń ze strony cyberświata ochrona danych jest obecnie zasadniczym elementem bezpieczeństwa.

1.2. Wzajemne oddziaływanie

Ponieważ funkcje bezpieczeństwa mogą przerywać ciągłość procesów produkcyjnych, zdarzają się liczne próby nielegalnego ich omijania, czemu w przeszłości zapobiegano poprzez zastosowanie środków mechanicznych. Przykładem takich działań było plombowanie śrub, które zapobiegało wymontowywaniu czujników bezpieczeństwa. Obecnie możliwe jest przeprowadzanie tego typu manipulacji, za pośrednictwem sieci. Jeśli na przykład maszyna pracuje w bezpiecznych warunkach dzięki kurtynie świetlnej, jej program można zmienić w taki sposób, aby określone dane przestały być brane pod uwagę. Funkcja bezpieczeństwa zostaje wówczas wyłączona, zaś maszyna pracuje nadal nawet w niebezpiecznych sytuacjach.
Z drugiej strony, mechanizmy zabezpieczające można również wykorzystać do uszkodzenia maszyn za pośrednictwem sieci w sposób celowy. W tym przypadku wystarczające jest zwyczajne przerwanie transferu danych. Ponieważ mechanizmy zabezpieczające cyklicznie sprawdzają, czy użytkownik sieci po przeciwnej stronie połączenia jest wciąż aktywny. Z chwilą wykrycia braku odpowiedzi maszyna zostaje zatrzymana. Jedną z opcji osiągnięcia zamierzonego efektu są wspomniane już ataki DoS, które wywołują przeciążenie sieci.

Za pośrednictwem sieci można nie tylko zakłócać procesy produkcyjne. Można również na przykład z powodzeniem generować inne zagrożenia. Celem hakerów są mechanizmy bezpieczeństwa sprawdzające, czy maszyna jest włączona, czy nie. Jeśli mechanizmy te zostają zmienione tak, że napęd pracuje w sposób nieprzerwany, może to prowadzić w najgorszym przypadku nawet do zniszczenia maszyny. Dlatego też urządzenia, takie jak turbiny wiatrowe, wyposażone są w podwójne, a nawet potrójne zabezpieczenia.

2. Znaczenie ochrony danych w automatyzacji

2.1. Cel

Stosowanie założeń platformy Industry 4.0, skupiających się głównie na podłączeniu instalacji do sieci, może stwarzać zagrożenia ze strony cyberświata, będące poważnym problemem dla firm produkcyjnych. Wszystkie procesy wykorzystujące technologię IT można skutecznie chronić, jednak jest to zadanie złożone i kosztowne. W związku z tym należy na początku przeprowadzić badania w celu stwierdzenia, z jakimi zagrożeniami ma się rzeczywiście do czynienia, a każda strategia musi być efektem analizy pod kątem wydajności przedsiębiorstwa.
Ochrona danych ma na celu zagwarantowanie dostępności sieci i urządzeń oraz integralności i poufności danych. W tym celu rozproszone systemy sterowania muszą być chronione nie tylko przed atakami DoS, ale również przed błędami oprogramowania, sprzętu i obsługi. Innym efektem manipulowania przesyłaniem lub przechowywaniem danych jest przerywania procesów produkcyjnych, co sprawia, że istotną rolę pełni integralność danych. Ponadto naruszenie poufności danych może powodować poważne konsekwencje, na przykład program aplikacji maszyny pada ofiarą szpiegostwa, po czym jest kopiowany.

2.2. Więcej niż bezpieczeństwo IT

Aby móc elastycznie reagować na różne scenariusze, obecnie wdraża się strategie zabezpieczeń zawierające kilka warstw ochrony: ich rdzeniem są podzespoły automatyzacji. Następnie jest sieć, za pośrednictwem której podzespoły te mogą komunikować się z innymi sieciami, np. z systemem ERP. Górną warstwą jest fabryka, która jest chroniona przed zewnętrznym światem przez system firewall.
Jednakże takie konfiguracje mogą okazać się niewystarczające dla pełnego zabezpieczenia instalacji, ponieważ zagrożenia mogą pochodzić również z wewnątrz zakładu. Fizyczne zabezpieczenie przed nieuprawnionym dostępem do urządzeń sieciowych, takich jak systemy firewall i przełączniki, są podstawą każdej strategii bezpieczeństwa. Jedynym sposobem uchronienia tych urządzeń przed manipulacją wewnątrz zakładu jest uniemożliwienie swobodnego dostępu do nich. Instalowanie urządzeń sieciowych zamykanych na kłódkę w szafach sterowniczych lub skrzynkach przyłączeniowych może być prostym i skutecznym rozwiązaniem. Jednocześnie można również istotnie ograniczyć ryzyko wystąpienia błędów w obsłudze wywołanych przez nieuprawnionych pracowników.

2.3. Wpływ na cykl eksploatacji instalacji

Cykl eksploatacji instalacji może wynosić 20 lub więcej lat. Obecnie najczęściej stosuje się zasadę „Nigdy nie wymieniaj pracującego systemu”. To oznacza, że gdy zachodziła konieczność aktualizacji mechanizmów zabezpieczających, sterownik był zazwyczaj wymieniany na nowy model tego samego typu. Ponieważ bezpieczeństwo funkcjonalne gwarantowane jest tak długo, jak długo maszyna nie podlega istotnym zmianom. Podstawą tego podejścia były statystyczne modele awarii, które pozwalały wyznaczyć prawdopodobieństwo wystąpienia uszkodzenia. I nic w tej dziedzinie nie zmieniało się wraz z upływem czasu.
Z drugiej strony, ochrona danych jest „celem ruchomym”. Inaczej niż w odniesieniu do bezpieczeństwa, ważne jest nie to, że usterka może wystąpić z prawdopodobieństwem na przykład 1:100 000, lecz to, że jeśli podmiot atakujący przedostanie się wcześniej do sieci, prawdopodobieństwo wyniesie 1:1. Ponadto coraz bardziej wyrafinowane metody obchodzenia zabezpieczeń są w stadium ciągłego rozwoju i algorytmy, które kiedyś gwarantowały bezpieczeństwo, obecnie przestają. Kilka lat temu powszechnie stosowanym standardem był Data Encryption Standard (DES), obecnie BSI (Niemiecki Urząd Federalny ds. Ochrony Informacji) nie zaleca stosowania go. To samo obowiązuje dla algorytmu kryptograficznego MD5. W przypadku wkroczenia komputerów kwantowych wkrótce stanie się możliwe wyliczenie kluczy kryptograficznych w ciągu kilku minut, a nawet sekund, co w przypadku obecnie pracujących komputerów musiałoby zająć stulecia.
Ponieważ ochrona danych nie jest parametrem fizycznym, lecz raczej „poruszającym się celem”, środki podejmowane przeciwko cyberzagrożeniom muszą być nieustannie aktualizowane. Odpowiedzialność za ten proces spoczywa głównie na właścicielach instalacji, dla których ochrona danych oznacza również ochronę własnych inwestycji. Stosując skuteczną strategię ochrony, można eksploatować instalację tak długo jak dawniej. Oprócz tego, producenci maszyn i podzespołów są zobowiązani do natychmiastowego poinformowania właścicieli instalacji w przypadku pojawienia się nowych problemów związanych z bezpieczeństwem oraz do zapewnienia aktualizacji oprogramowania dla ich urządzeń, dzięki którym możliwe będzie wyeliminowanie słabych elementów instalacji. Wymaga to jednak ścisłej współpracy obu stron na przestrzeni całego cyklu produkcyjnego.

3. Formy zagrożeń

3.1. Ataki zewnątrzne

Sieci automatyzacji oparte na protokole Ethernet są narażone na zagrożenia, które można podzielić na kategorie w zależności od ich pochodzenia. Przede wszystkim istnieją ataki zewnętrzne i wewnętrzne oraz niezamierzone naruszenia zabezpieczeń, dla których różne są motywy.
Jeśli sieci są połączone ze środowiskiem zewnętrznym, ma to zazwyczaj związek ze złośliwymi działaniami mającymi cechy sabotażu wobec instalacji.
Innym zagrożeniem mogącym mieć ujemne następstwa jest szpiegostwo przemysłowe. Jeśli na przykład zostanie wykradziona informacja na temat produktów lub wiedzy na temat procesu produkcyjnego, wówczas na potencjalne ryzyko narażona jest konkurencyjność przedsiębiorstwa. To samo ma miejsce również wówczas, gdy zostają wykradzione poufne dane finansowe lub informacje o klientach, przetargach czy zamówieniach.

Aby uzyskać dostęp do haseł i danych logowania, atakujący wykorzystują czasami idealnie skopiowane witryny internetowe i wiadomości e-mail, stosując tak zwany phishing. Jeśli odbiorcy nie wykazują czujności, atakujący ma zdecydowanie ułatwioną sytuację. Dlatego tak ważne jest, aby przedsiębiorstwa podnosiły świadomość pracowników w dziedzinie ochrony danych i ustalały wytyczne obowiązującego każdego pracownika.
W ostatnim czasie zanotowano zwiększoną liczbę ataków o charakterze przestępczym. Ta metoda nosi nazwę oprogramowania szantażującego (ransomware), które może być ukryte w plikach programów np. Word, PowerPoint lub Excel przesyłanych jako załączniki do wiadomości e-mail. Po otwarciu przez adresata tych plików w jego komputerze zostają zaszyfrowane wszystkie pliki. Takie złośliwe oprogramowanie może również rozprzestrzeniać się na inne urządzenia w sieci. Jedynym sposobem odzyskania dostępu do swoich danych jest zapłacenie okupu.

3.2. Ataki wewnętrzne

Mimo że informacje o atakach zewnętrznych pojawiają się wciąż w czołówkach gazet, to równie niebezpieczne są ataki wewnątrz sieci. W tym przypadku można dosłownie obejść strategie zabezpieczające. Intencje atakujących są zasadniczo takie same, różne jest tylko podejście. Jedna z możliwych opcji polega na tym, że atakujący wchodzą do firmy i poszukują wolnego łącza w sieci Ethernet w celu wprowadzenia do niej szkodliwego oprogramowania. Wystarczy do tego mała pamięć USB, której nie można wykryć podczas kontroli przy wchodzeniu do zakładu.
Częściej jednak atakujący wykorzystują fakt, że najsłabszym ogniwem w zakresie ochrony danych są ludzie. Skuteczną metodą manipulowania pracownikami jest tak zwana inżynieria społeczna. Jej celem jest pozyskanie zaufania pracowników i wykorzystanie ich jako użytecznych narzędzi.

3.3. Nieumyślne naruszenie zabezpieczeń

Jednak większość cyberincydentów nie jest związana ani z zewnętrznymi, ani wewnętrznymi atakami, lecz nieumyślnymi działaniami, których konsekwencje mogą być równie poważne, jak w przypadku pozostałych dwóch scenariuszy. Mogą one prowadzić do awarii sieci lub rozpowszechniania wrażliwych informacji, poprzez niewłaściwie skonfigurowane urządzenia oraz błędy obsługi.
Dlatego też pracownicy produkcyjni niebędący zazwyczaj ekspertami w dziedzinie IT, muszą zostać odpowiednio przeszkoleni. Ponadto sieci powinny zostać tak skonfigurowane, aby zminimalizować efekty spowodowane przez nieprawidłowo skonfigurowane lub obsługiwane urządzenia – poprzez np. segmentację, tzn. podział instalacji na podsieci oraz stosowanie różnych środków bezpieczeństwa.

4. Ocena poziomu bezpieczeństwa

4.1. Podstawy normatywne

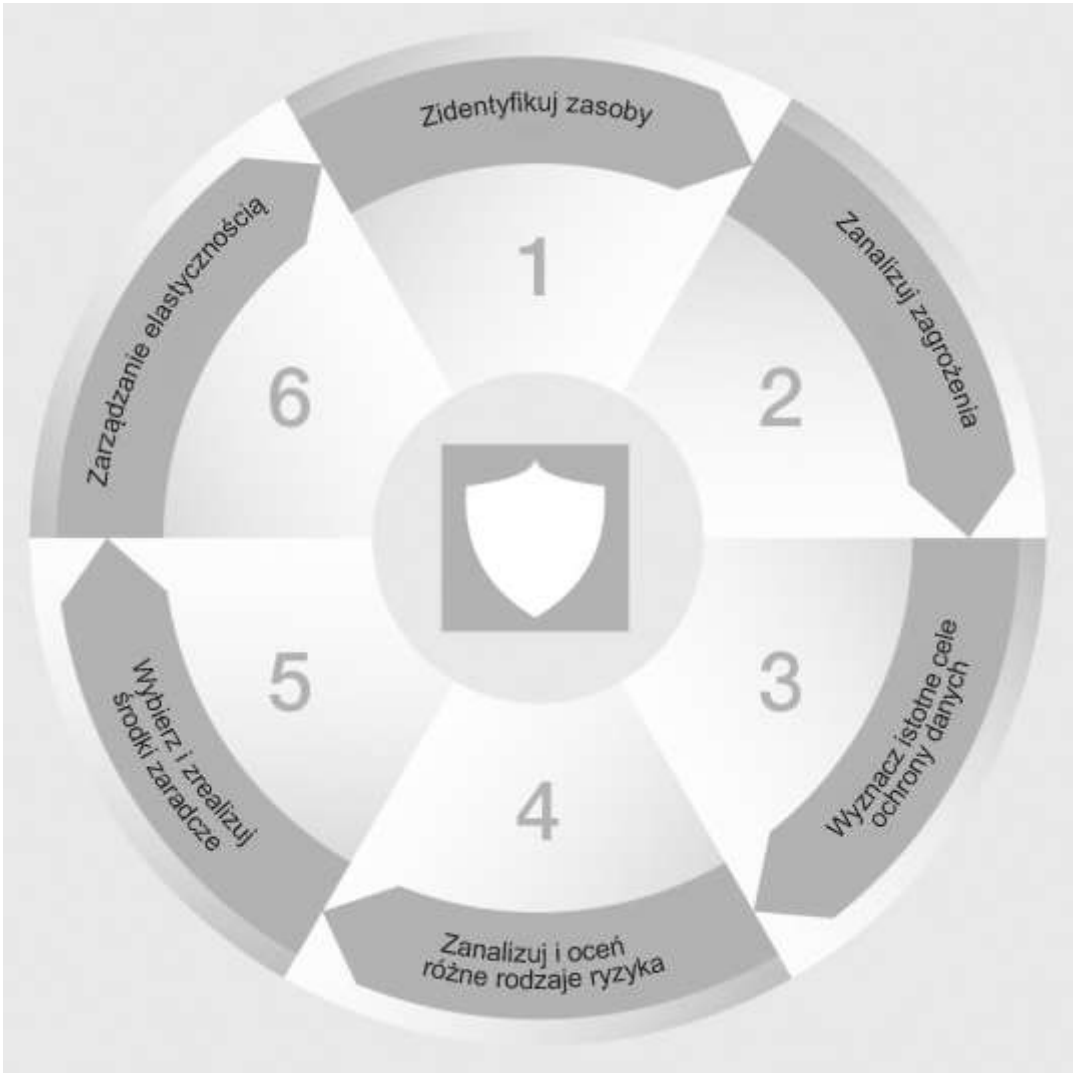
Przez wiele lat bezpieczeństwo pełniło podstawową rolę w technologii IT, i właśnie dlatego istnieje szereg norm takich jak np. PN-ISO/IEC 27000 Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Przegląd i terminologia. W odniesieniu do automatyzacji wymagań tych jednak nie można zastosować. Tutaj największe znaczenie ma przede wszystkim dostępność danych i jest to krytyczny warunek wstępny dla płynności procesów produkcyjnych, podczas gdy w technologii IT priorytet ma poufność danych.
Aby umożliwić wprowadzenie skutecznych rozwiązań ochrony danych w automatyzacji, szereg różnych organizacji przystąpiło do opracowania odpowiednich norm. Jednak opisują one wyłącznie częściowe aspekty, takie jak rozróżnienie pomiędzy ochroną i bezpieczeństwem. Oprócz tego, nie są one dostępne jako oficjalne dokumenty, lecz służą bardziej jako referencje techniczne.
Dzięki normie PN-EN IEC 62443 „Bezpieczeństwo w systemach sterowania i automatyki przemysłowej" powstała międzynarodowa seria norm, z których część została już przyjęta i które szczegółowo opisują bezpieczeństwo IT w automatyzacji.

Rysunek 1: Norma PN-EN IEC 62443

Zakres omawianych zagadnień rozciąga się od analizy ryzyka, poprzez najlepsze praktyki inżynierskie, po projektowanie bezpiecznych produktów (bezpieczeństwo danych dzięki bezpiecznej konstrukcji). W rezultacie norma PN-EN IEC 62443 przedstawia aktualnie najlepszą wiedzę na potrzeby operatorów instalacji i producentów maszyn dla efektywnego wdrażania ochrony danych.
„Kompendium ochrony danych ICS" opracowane przez Niemieckie Federalne Biuro na rzecz bezpieczeństwa informacji (BSI) skierowane jest w szczególności do operatorów przemysłowych systemów sterowania. Wyjaśnione w nim nie tylko ogólne zasady, ale też szczególne wymagania oraz postanowienia najważniejszych norm. Ponadto przedstawiono odpowiednie środki i sposoby ich realizacji.
Podczas gdy norma PN-EN IEC 62443 oraz „Kompendium ochrony danych ICS" przeznaczone są głównie dla specjalistów z branży automatyki, dyrektywa VDI/VDE 2182 jest bezpośrednim wprowadzeniem do tego zagadnienia. Oprócz tego wiele przedsiębiorstw działających w sektorze automatyzacji opublikowało własne materiały. Z racji złożoności zagadnień bezpieczeństwa przemysłowego do projektów zaleca się angażować specjalistów z zewnątrz – najpóźniej w momencie rozpoczęcia realizacji.

4.2. Analiza ryzyka

Podobnie jak każda inna strategia, strategia ochrony danych rozpoczyna się od oceny sytuacji, co oznacza, że operatorzy instalacji muszą najpierw zrozumieć, na jakie zagrożenia mogą być



Rysunek 2: Etapy projektu analizy ryzyka

narażeni i na ochronie jakich wartości przedsiębiorstwa muszą się skoncentrować. Następnie należy zdefiniować pięć poziomów bezpieczeństwa, od 0 (brak ryzyka) do 5 (maksymalne ryzyko). Jednak nigdzie nie zostało opisane, jak te wymagania spełnić.

Ochrona bezpieczeństwa	Ochrona
SL 0	Brak ochrony
SL 1	Ochrona przed przypadkowym naruszeniem
SL 2	Ochrona przed umyślnym naruszeniem z użyciem prostych środków
SL 3	Ochrona przed umyślnym naruszeniem z użyciem zaawansowanych środków
SL 4	Ochrona przed umyślnym naruszeniem z użyciem zaawansowanych środków oraz rozbudowanych zasobów

Rysunek 3: Ocena ryzyka

Generalnie wszystkie urządzenia posiadające łącze Ethernet można uznać za narażone na ryzyko, gdyż mogą one zostać wykorzystane jako bramka do ataków zarówno z zewnątrz, jak i od wewnątrz lub mogą być pierwszym elementem narażonym na nieumyślne naruszenia zabezpieczeń. Jeśli w urządzeniach tych zainstalowane są dodatkowo najpopularniejsze systemy operacyjne, wówczas ryzyko to jest większe. W szczególności, gdy aktualizacje tych systemów pod kątem bezpieczeństwa nie są wykonywane regularnie.
Przeprowadzona analiza ryzyka zawsze dotyczy tylko stanu bieżącego. W dowolnej chwili mogą pojawić się nowe zagrożenia, które należy wziąć pod uwagę. Jeśli na przykład procesory nie były poprzednio uznawane za krytyczne, to w ostatnim czasie wykryto w nich luki, którym nadano przydomki „Meltdown” i „Spectre” i które czynią wiele komputerów podatnymi na ataki. Obecnie obiektem ataków hakerów stają się coraz częściej programowalne sterowniki PLC. Podsumowując: ochrona danych jest procesem ciągłym, wymagającym stałej analizy i wytrwałości.

4.3. Środki zaradcze

Po zdefiniowaniu i nadaniu priorytetów wartościom przedsiębiorstwa, które muszą być bezwzględnie chronione – udany atak na sterownik wiąże się zazwyczaj z o wiele poważniejszymi konsekwencjami niż atak na narzędzie wizualizacji – konieczne jest podjęcie decyzji co do metody zabezpieczenia się przed tymi zagrożeniami.
Idealnym rozwiązaniem jest zapobieganie atakom oraz niezamierzonym naruszeniom bezpieczeństwa, zanim one nastąpią. Jednak w związku z kompleksowością i dynamicznym charakterem przedmiotu nie zawsze jest to możliwe do zrealizowania. Nawet jeżeli zostaną zatrudnieni specjaliści do stałego wyszukiwania nowych słabych punktów sieci, nie można całkowicie zabezpieczyć się przed każdą ewentualnością ataku.
Gdy już do niego dojdzie, należy natychmiast rozpoznać problemy związane z bezpieczeństwem i od razu zareagować. W tym celu niezbędne jest rejestrowanie wszystkich

zdarzeń zachodzących w sieci, a także ich szczegółowa analiza. Dzięki czemu można na przykład ustalić moment dostępu do określonego urządzenia. Jeśli na przykład prace konserwacyjne były wykonywane o nietypowej porze, wówczas powinno to zwrócić naszą baczną uwagę. Jeśli atak powiódł się lub nieumyślnie została naruszona ochrona danych, wówczas należy jak najszybciej rozwiązać problem i przeanalizować jego przyczyny, w taki sposób aby nie dopuścić do ponownego powtórzenia się takiej sytuacji w przyszłości.

5. Wdrażanie strategii ochrony

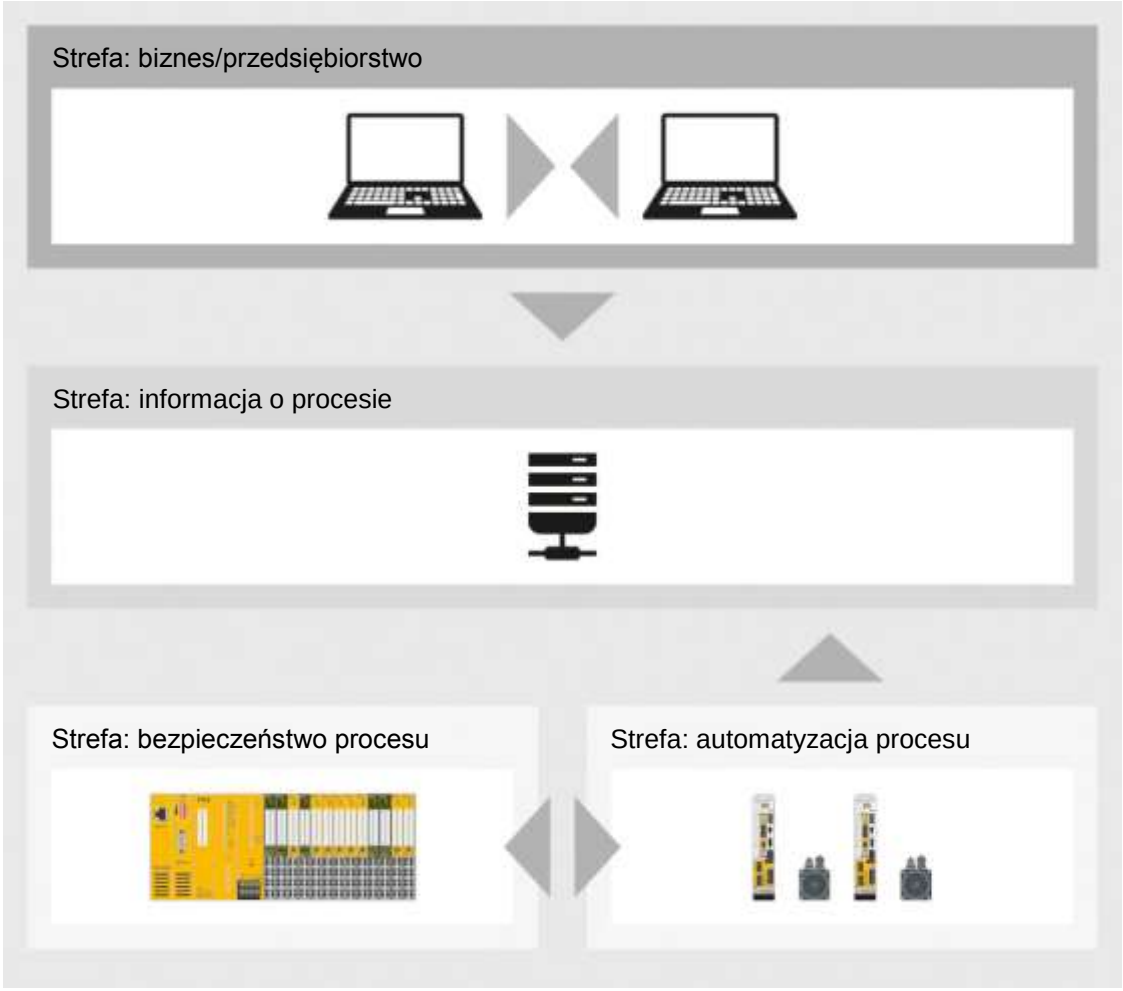
5.1. Systemy Firewall

Środkiem służącym do wdrażania strategii ochrony danych jest zabezpieczenie sieci za pomocą specjalnych urządzeń. Nawet jeśli rutery i przełączniki posiadają mechanizmy zabezpieczające, to jednak systemy firewall odgrywają ważną rolę. Chodzi tu zarówno o rozwiązania programowe, jak i sprzętowe (połączenie sprzętu i oprogramowania) monitorujące cały przepływ danych bazujących na zdefiniowanych indywidualnie regułach i realizujących takie funkcje jak głęboka kontrola pakietów lub wykrywanie włamań.
Systemy firewall wymagają zazwyczaj skomplikowanej konfiguracji, wymagającej posiadania rozległej wiedzy z dziedziny IT, którą nie dysponują pracownicy sektora produkcyjnego. Firma Pilz oferuje łatwy w uruchomieniu przemysłowy system firewall SecurityBridge, który pozwala nie tylko skutecznie chronić przed atakami i nieuprawnionym dostępem systemy sterowania firmy Pilz, ale również przesyłać dane procesowe o krótkim czasie opóźnienia.
Jednak, aby urządzenia zabezpieczające spełniały swoje zadania muszą ona zostać zaprojektowane w sposób bezpieczny na każdym poziomie, a aspekt ten należy uwzględniać na przestrzeni całego cyklu eksploatacji. Jak ważny jest to aspekt pokazują błędy sprzętowe Meltdown i Spectre. Istnieje również możliwość wprowadzenia złośliwego oprogramowania do procesu produkcyjnego, w celu wykorzystania go jako furtka do ataków. Aby do tego nie dopuścić, producenci maszyn muszą stale monitorować cyberświat pod kątem nowych zagrożeń i – w razie potrzeby – wyposażać swoje urządzenia w dodatkowe mechanizmy zabezpieczające i stale je aktualizować.

5.2. Segmentacja sieci

Systemy Firewall są zazwyczaj umieszczane na styku pomiędzy siecią bezpieczną i niebezpieczną, na przykład pomiędzy intranetem i internetem. Jednak ta tak zwana ochrona graniczna szybko natrafia na ograniczenia, gdy jej zadaniem jest niedopuszczenie do rozprzestrzeniania się złośliwego oprogramowania po całej sieci.

Dlatego też norma PN-EN IEC 62443 wymaga podzielenia sieci na sekcje, zgodnie z modelem „Strefy i kanały”.

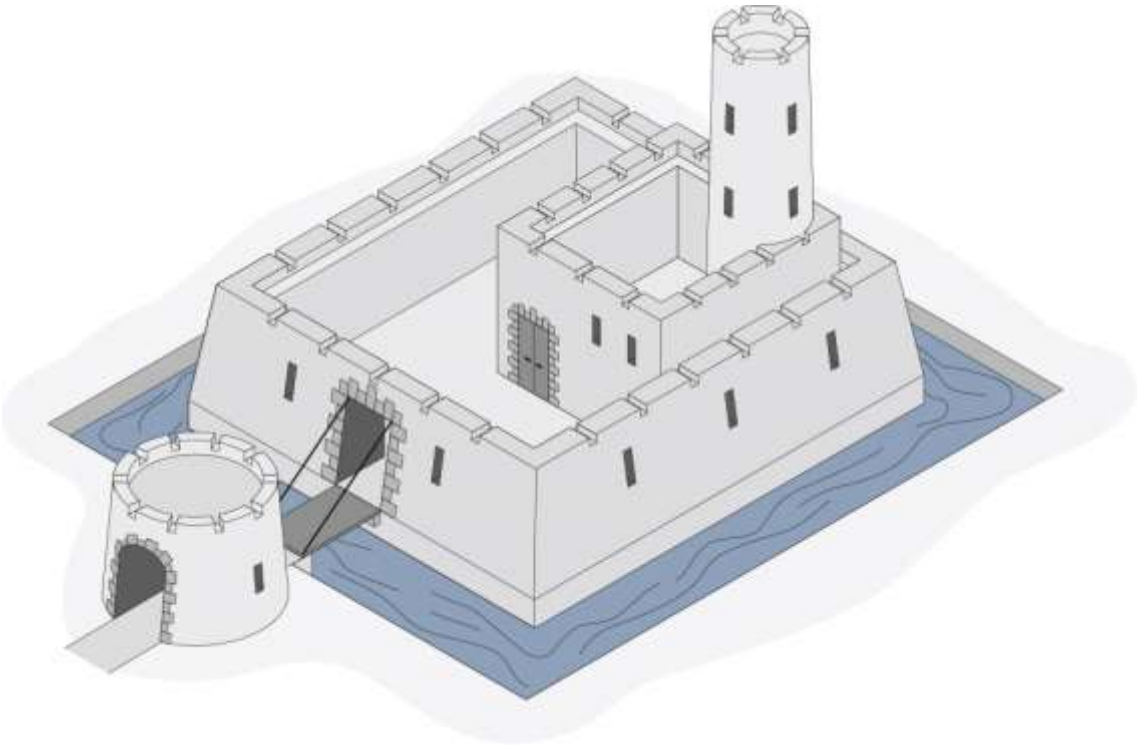


Rysunek 4: Model „Strefy i kanały”

Model ten umożliwia oddzielenie sieci administracyjnych od produkcyjnych. W razie potrzeby sieci te można rozbić na segmenty, aż po pojedyncze komórki wytwórcze. Strefy wejściowe, w których urządzenia charakteryzują się podobnymi wymaganiami dotyczącymi bezpieczeństwa są identyfikowane, a następnie oddzielane od siebie za pomocą systemu firewall lub bezpiecznych ruterów. Dzięki czemu wyłącznie urządzenia, które są do tego upoważnione, mogą wysyłać i odbierać informacje za pośrednictwem kanałów pomiędzy strefami.
Co to oznacza w praktyce, pokazuje przykład: nieumyślne naruszenia bezpieczeństwa spowodowane są często przez nieprawidłowo skonfigurowane urządzenia. Konsekwencją tego może być przesyłanie danych, które mogą ujemnie wpłynąć na inne urządzenia. Jeśli jednak sieci podzielone są na chronione podsieci, wówczas problemem tym dotknięte są wyłącznie urządzenia w ramach jednej strefy, w której ten problem wystąpił. Dotyczy to również skutków niezamierzonego lub złośliwego dostępu od wewnątrz.

5.3. Obrona głęboka

Aby maksymalnie utrudnić pracę hakerom, model „Strefy i kanały” można wykorzystać również jako element centralny dla głębokiej ochrony sieci. Zasada ta wykorzystywana jest w budowie fortyfikacji, opiera się na ciągłym stawianiu nowych i zróżnicowanych przeszkód na drodze intruzów. W średniowieczu zamki chronione były przez fosę, zapadnie, mosty zwodzone, wieże i kilka rzędów murów.
Strefy i kanały w sieci odpowiadają bramom zamkowym. Mury i inne przeszkody składają się z systemów firewall i bezpiecznych ruterów obsługujących różne mechanizmy zabezpieczające. Obejmują one na przykład kontrole dostępu zgodnie z IEEE 802.1x oraz listy kontroli dostępu, blokujące nieznane urządzenia i protokoły. Oprócz tego istnieją mechanizmy wyzwalające alarmy w przypadku wystąpienia podejrzanej aktywności lub wykrywają czy przesyłane są pakiety IP z fałszywymi adresami nadawców (podszywanie się pod nadawcę).
Dzięki temu jedna metoda ataku sama w sobie nie prowadzi do „sukcesu”. Aby móc



Rysunek 5: Poziomy ochrony na przykładzie obrony zamku

przemieszczać się w głąb sieci, haker musi wciąż pokonywać nowe, zachodzące na siebie warstwy ochronne. I nawet gdyby udało mu się przedostać się przez podsieci komórki produkcyjnej, niemożliwe okaże się zaatakowanie stamtąd celów zlokalizowanych w sąsiadujących podsieciach.

5.4. Środki organizacyjne

To, czy przedsiębiorstwa produkcyjne zabezpieczają się przed zagrożeniami ze strony cyberświata, jest zawsze wynikiem porównania kosztów z zyskami. Na przykład w Niemczech ustawa o bezpieczeństwie IT obliguje operatorów infrastruktury o ogólnym znaczeniu społecznym, na przykład działających w sektorach energetycznych, komunikacji czy zdrowia do wdrożenia odpowiednich rozwiązań bezpieczeństwa. Inne kraje mają również porównywalne specyfikacje prawne, na przykład w USA dotyczą one ochrony sieci energetycznych.
W odpowiedzi na pojawiające się liczne zagrożenia utworzono wiele jednostek wspierających ochronę instalacji przed umyślnym i nieumyślnym naruszeniem bezpieczeństwa danych. Nawet zaawansowane koncepcje systemu firewall nie są wystarczające same w sobie.
Ważne jest, aby to całe przedsiębiorstwo uczestniczyło w ochronie danych. Ponadto konieczne jest ustanowienie wytycznych nie tylko obowiązujących pracowników, ale również producentów urządzeń i dostawców usług.
Oprócz tego ważne jest, aby specjaliści w dziedzinie IT i automatyzacji ściśle z sobą współpracowali, co oznacza, że muszą oni poznać zróżnicowane wymagania drugiej strony, a także jej tryby pracy. Konieczne jest również powołanie organizacji, której członkowie byliby odpowiedzialni za ochronę danych w sektorze produkcyjnym oraz ich ciągłe usprawnienia. Na jej czele powinien stać członek kadry kierowniczego lub przynajmniej jego zastępca.

5.5. Szkolenia

„Jeśli przestaniesz się doskonalić, cofniesz się” to przepis na sukces, który również przedsiębiorstwa powinny stawiać sobie za cel w odniesieniu do ochrony danych. Tę możliwość oferują regularne kursy szkoleniowe dotyczące zagadnień bezpieczeństwa i ochrony danych. Mają one na celu zwiększanie świadomości pracowników. Powinny obejmować zagadnienia dotyczące aktualnych zagrożeń oraz wskazówki, jak należy wypełnić luki w zabezpieczeniach. Pozwoli to zapobiegać zagrożeniom wynikającym z błędnych decyzji, spowodowanych niewystarczającymi kwalifikacjami pracowników.
Szkolenia organizowane prze firmę Pilz są w szczególności skierowane do projektantów maszyn i instalacji. Zapewniają dokładny przegląd zagadnień bezpieczeństwa i ochrony, a także wyjaśniają, jak rozpoznać zagrożenia i jak je zminimalizować. Zakres tematów obejmuje architekturę sieci, uwierzytelnianie abonentów sieci oraz szyfrowanie danych, a także bezpieczną zdalną konserwację.

6. Podsumowanie i prognozy

Aby osiągnąć możliwie najwyższy poziom ochrony danych, najważniejsze jest dokładne poznanie architektury sieci, a także protokołów komunikacyjnych oraz rodzaju transmisji danych. Jest to jedyny sposób uniknięcia zagrożeń zarówno z zewnątrz, jak i od wewnątrz, umyślnych czy też nieumyślnych.
W przeszłości bezpieczeństwo danych odnosiło się niemal wyłącznie do klasycznej technologii IT. Ponieważ produkty seryjne z sektora konsumenckiego oraz złożone systemy operacyjne są obecnie powszechnie wykorzystywanie w instalacjach produkcyjnych jako element platformy Industry 4.0, konieczne stało się, aby również automatyzacja uwzględniała ten aspekt.

Brak możliwości wiernego zaadoptowania norm pochodzących z branży IT, opracowano nowe normy na potrzeby branży automatyzacji, z których najważniejszą jest PN-EN IEC 62443. Definiuje ona sposób opracowania i wdrożenia krok po kroku ogólnej strategii ochrony danych dla sektora przemysłowego.
Strategie te muszą uwzględniać zagadnienia bezpieczeństwa, gdyż ich funkcjonowanie można zagwarantować wyłącznie w przypadku niezawodnego przesyłania odpowiednich danych. Zagrożenia bezpieczeństwa danych mogą się wciąż zmieniać, a wraz z nimi będą zmieniać się środki zaradcze. Oznacza to, że nawet jeśli oba aspekty automatyzacji pozostaną niezależne, to muszą one być z sobą ściśle zharmonizowane. Dobra wiadomość: Doświadczony znawca zagadnienia bezpieczeństwa łatwiej opanuje tematykę ochrony danych, ponieważ podejścia te są zbieżne.

Glosariusz

Lista kontroli dostępu	Lista kontroli dostępu (ACL) definiuje zakres, w którym pojedyncze osoby, komputery lub sieci są upoważnione do użytkowania określonych serwisów w celu uzyskania dostępu do rutera lub przełącznika. Możliwe jest zdefiniowanie dostępu dla pojedynczych komputerów lub sieci, a także odpowiednich metod dostępu.
Burza broadcastowa	Burza broadcastowa oznacza duże skumulowanie ruchu nadawczego w sieci komputerowej, w wyniku czego przestaje być możliwe ustanowienie jakichkolwiek połączeń sieciowych i możliwe jest przerwanie połączeń już istniejących. Burza broadcastowa może być spowodowana przez atak, nieprawidłową konfigurację lub nawet nieodpowiednie zaprojektowanie sieci.
Głęboka inspekcja pakietów	Głęboka inspekcja pakietów jest to procedura w technologii sieciowej służąca do monitorowania i filtrowania pakietów danych. Za jej pośrednictwem możliwe jest zwalczanie spamu i można ją również wykorzystać do sprawdzania przeciążenia i zmniejszenia ruchu danych.
DES (Standard szyfrowania danych)	Standard szyfrowania danych lub w skrócie DES jest to unormowana metoda symetrycznego szyfrowania.
Algorytm MD5	Algorytm kryptograficzny MD5 (Message Digest Algorithm 5) należy do grupy matematycznych funkcji jednokierunkowych. Oznacza on, że nie istnieje łatwy sposób wykorzystania wyniku do zidentyfikowania parametru wejściowego. Z wykorzystaniem algorytmu MD5 każda ilość danych wejściowych zawiera się w wartości o długości 128 bitów. Stosowanie algorytmu MD5 pozwala założyć, że byłoby niezwykle trudno znaleźć dwa dokumenty wejściowe prowadzące do tej samej wartości wynikowej (kolizja). Stosowanie algorytmu MD5 przez długi czas pozwalało identyfikować słabe punkty umożliwiające hakerowi tworzenie kolizji.
System wykrywania włamań	Wykorzystując system wykrywania włamań, ataki skierowane na system komputerowy lub sieć komputerów, można szybko rozpoznać i zainicjować środki zaradcze.
Podszywanie się pod nadawców	Podszywanie się pod nadawców odnosi się do podrabiania adresów nadawców pakietów IP w sieciach komputerowych, w celu wykorzystania fałszywej tożsamości, aby oszukać atakowany system IT. Każdy pakiet IP zawiera adres nadawcy umieszczony w danych nagłówka. Haker może sfałszować adres nadawcy w danych nagłówka, tak, aby wyglądało to na wysłanie pakietu z innego komputera. Wiele protokołów z rodziny TCP/IP może być uwierzytelnianych wyłącznie za pośrednictwem adresu IP. W przypadku jego sfałszowania możliwe jest oszukanie środków ochrony danych takich jak uwierzytelnianie oparte na adresie IP w sieci. Podszywanie się pod nadawców jest jednym z rodzajów

	podszywania się. Obecnie pod pojęciem „podszywania się” rozumie się wszystkie metody, za pomocą których można obejść proces uwierzytelniania i identyfikacji, wykorzystując wiarygodne adresy lub nazwy hostów protokołów sieciowych.
Meltdown i Spectre	Meltdown i Spectre są to luki w zabezpieczeniach wykryte w mikroprocesorach, za pośrednictwem których możliwe jest uzyskanie nieuprawnionego dostępu do pamięci zewnętrznych procesów.
Standard sieciowy IEEE 802.1x	IEEE 802.1X jest to standard sieciowy służący do uwierzytelniania użytkowników w sieciach IEEE-802. Standard ten działa jak jednostka nadrzędna sprawdzająca użytkownika, zanim uzyska on dostęp do sieci LAN lub WLAN.
Cel ochrony: Integralność	Integralność danych oznacza, że dane i tryb pracy systemu są zawsze prawidłowe. W przypadku zagwarantowania integralności możliwe jest wykrywanie nieupoważnionych lub niewykrytych zmian i natychmiastowe ich wyeliminowanie.
Segmentacja sieci	Segmentacja oznacza podział sieci na mniejsze jednostki. Jednostki te są następnie łączone ze sobą za pośrednictwem systemu firewall lub innych urządzeń, z którymi komunikacja może być ograniczona. Zatem możliwe jest ograniczenie wpływu burz broadcastowych i innych „niezamierzonych” zdarzeń, a także skutków ataków.

Wykaz rysunków

Nasze oddziały znajdziesz na całym świecie. Więcej informacji znajdziesz na naszej stronie internetowej www.pilz.pl lub kontaktując się z naszą siedzibą główną.

Siedziba główna: Pilz GmbH & Co. KG, Felix-Wankel-Straße 2, 73760 Ostfildern, Niemcy
Telefon: +49 711 3409-0, Faks: +49 711 3409-133, e-mail: info@pilz.de
www.pilz.com

PILZ
THE SPIRIT OF SAFETY