Przewodnik cyberbezpieczeństwa dla przedsiębiorstw

Platforma Przemysłu Przyszłości

KRZYSZTOF MIZERSKI

Ekspert współpracujący z Platformą Przemysłu Przyszłości

Ryzyko wynikające z cyberzagrożeń jest jednym z najpoważniejszych problemów współczesnych przedsiębiorstw. Każdy podmiot, który wykorzystuje poufne dane oraz korzysta z rozwiązań IT, bez względu na wielkość, obszar czy profil działalności, jest realnie zagrożony możliwością strat z tytułu cyberataków. Co więcej, ryzyko zwiększa się wraz z rozwojem danej organizacji w zakresie wykorzystania nowoczesnych technologii.

Wstęp

Ryzyko wynikające z cyberzagrożeń jest jednym z najpoważniejszych problemów współczesnych przedsiębiorstw. Każdy podmiot, który wykorzystuje poufne dane oraz korzysta z rozwiązań IT, bez względu na wielkość, obszar czy profil działalności, jest realnie zagrożony możliwością strat z tytułu cyberataków. Co więcej, ryzyko zwiększa się wraz z rozwojem danej organizacji w zakresie wykorzystania nowoczesnych technologii. Do podstawowych źródeł występowania cyberryzyka należy wykorzystanie technologii IT, systemów IT oraz korzystanie z sieci komputerowej. Najsłabszym ogniwem, który często decyduje o podatności danej instytucji na cyberatak, są ludzie, którzy pracują przy obsłudze wymienionych systemów. Straty finansowe oraz problemy długookresowe, wynikające z cyberataków mają wpływ na sytuację ekonomiczną przedsiębiorstw, co w konsekwencji rzutuje na całą gospodarkę. Jakie działania są zatem konieczne, aby skutecznie ograniczyć ryzyko związane z cyberzagrożeniami? Jak zapewnić swojej firmie cyberbezpieczeństwo? O tym i nie tylko w dalszej części przewodnika.

Czym jest cyberbezpieczeństwo?

Cyberbezpieczeństwo — zgodnie z ustawą o krajowym systemie cyberbezpieczeństwa, jest to „odporność systemów informacyjnych na wszelkie działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy” (art. 2 pkt 4) Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2018 r. poz. 1560)). Warto zastanowić się, co oznacza podana definicja dla praktyki zarządzania przedsiębiorstwem.

W praktyce, systemy informacyjne firmy to po prostu używane w tej firmie serwery, komputery, telefony, tablety (i inne podobne urządzenia przenośne) wraz z oprogramowaniem służącym do ich używania, połączone siecią teleinformatyczną, oraz dane, które są przetwarzane za pomocą tych systemów.

Zapewnienie poufności danych oznacza zagwarantowanie, że dane nie będą ujawnione w sposób nieautoryzowany. Z kolei integralność danych oznacza ich kompletność i dokładność. Dostępność danych oznacza, iż nie została naruszona możliwość autoryzowanego dostępu do zasobów cyfrowych. Natomiast autentyczność danych jest to pewność, że przetwarzane dane są prawdziwe, tj. są danymi, które w sposób autoryzowany zostały wprowadzone do systemu.

Ograniczenie ryzyka, wynikającego z cyberzagrożeń oraz zapewnienie warunków bezpieczeństwa cyfrowego w obrębie przedsiębiorstwa wymaga przeprowadzenia przemyślanych, wieloetapowych działań oraz znajomości podstawowych zasad cyberbezpieczeństwa.

Niniejszy przewodnik stanowi zbiór zaleceń i najlepszych praktyk w obszarze cyberbezpieczeństwa dla współczesnych przedsiębiorstw. Jest kierowany w szczególności do małych i średnich firm, które nie dysponują odpowiednimi zasobami, aby powołać profesjonalny zespół do zarządzania cyberbezpieczeństwem wewnątrz swojej organizacji. Stanowi dość obszerny zasób zaleceń i rekomendacji, które mogą pomóc w dopasowaniu strategii cyberbezpieczeństwa firmy do charakteru swojej działalności. Skuteczne wdrożenie zaproponowanych rozwiązań pozwoli uniknąć wielu powszechnych incydentów bezpieczeństwa oraz zapewni ochronę kluczowych zasobów przedsiębiorstwa. Przewodnik,

poza propozycją podstawowych działań zapewniających cyberbezpieczeństwo, zawiera także dodatkowe zalecenia, oferujące jeszcze wyższy poziom ochrony zasobów i danych. Zaprezentowane wytyczne mogą stanowić punkt wyjściowy dla opracowania indywidualnej strategii cyberbezpieczeństwa dla współczesnych przedsiębiorstw.

Cyberbezpieczeństwo w każdej firmie — bez względu na jej wielkość czy charakter działalności — powinno być traktowane jako priorytetowa inwestycja w jej bezpieczeństwo i bezpieczeństwo biznesu, a nie jako koszt. Menedżerowie wyższego szczebla muszą zapewnić, aby cała kadra menadżerska uwzględniała kwestie cyberbezpieczeństwa w decyzjach dotyczących produktów, klientów, zasobów ludzkich i zamówień. Ponadto Kadra zarządzająca musi dbać o to, aby priorytety dotyczące cyberbezpieczeństwa zostały uwzględnione w wewnętrznych procedurach i codziennym funkcjonowaniu firmy we wszystkich jego obszarach.

Cyberbezpieczeństwo należy traktować jako swego rodzaju cykl, a nie jako proces przebiegający od pewnego początku do końca. Podstawą zapewnienia rzeczywistego zabezpieczenia systemów informatycznych (zarówno IT, OT jaki i IoT) jest uwzględnienie aspektów cyberbezpieczeństwa w każdym działaniu związanym z jego budowaniem rozpoczynając od procesu projektowania i planowania. Takie podejście — zwane „security by design” — powinno być elementem integralnym budowania każdego systemu informatycznego zarówno z punktu widzenia urządzeń, jak i całej infrastruktury. Cyberbezpieczeństwo powinno być warunkiem istnienia i jedną z podstawowych elementów każdego systemu informatycznego. Koncepcja „Security by design” odnosi się to do ciągłego podnoszenia poziomu bezpieczeństwa na każdym etapie rozwoju inteligentnego systemu produkcyjnego, czyli analizy, projektowania, wdrażania, testowania, eksploatacji i konserwacji.

Najlepsze praktyki i wytyczne dla przedsiębiorstw w zakresie zapewnienia cyberbezpieczeństwa wyrażono w formie wskazówek i zaleceń, które należy stosować w sposób indywidualny i dopasowany do charakterystyki działalności danej organizacji:

1. Zidentyfikuj kluczowe obszary zapewnienia ochrony:

W celu zapewnienia podstawowej ochrony:

- Określ, jakie dane i informacje posiada twoja firma i które z nich są kluczowe dla jej prawidłowego funkcjonowania
- Zidentyfikuj najważniejsze procesy wewnętrzne oraz oceń wpływ wykorzystania technologii teleinformatycznych na ciągłość tych procesów
- Sprecyzuj obszary, które generują największe ryzyko, związane z cyberzagrożeniami
- Bądź świadomy zagrożeń wynikających z cyberprzestrzeni oraz określ swoje słabe punkty
- Wyposaż nawet najbardziej podstawowe inteligentne urządzenia (zwłaszcza te o ograniczonych możliwościach procesora i pamięci jak np. czujniki, aktuatory) w funkcje wzajemnej identyfikacji i uwierzytelniania oraz zapewnij zgodność z rozwiązaniami typu Identity & Access Management.

W celu zapewnienia zaawansowanej ochrony:

- Przeprowadź inwentaryzację sprzętu, w celu określenia, jakie zasoby sprzętowe posiada twoja firma
- Dokonaj inwentaryzacji w zakresie wykorzystywanego oprogramowania i aktualnych wersji użytkowanych programów
- Przeanalizuj wspólnie z działem prawnym możliwe konsekwencje utraty danych, wycieku informacji oraz przerw w działalności na skutek cyberataków
- Zweryfikuj funkcjonowanie rozwiązań technicznych i organizacyjnych w swojej firmie za pomocą audytu bezpieczeństwa.
- Skoncentruj się na zapewnieniu odporności systemów Przemysłu 4.0 poprzez stworzenie planu ciągłości działania BCP (ang. *Business Continuity Planning*) i planu odtwarzania po awarii DRP (ang. *Disaster Recovery Plan*). Regularnie testuj plany bezpieczeństwa i dostosowuj je do wniosków wyciągniętych z testów i rzeczywistych incydentów bezpieczeństwa.
- Zdefiniuj krytyczne procesy biznesowe i technologiczne oraz określ, w jakim stopniu wpływają one na ciągłość biznesową, która musi zostać utrzymana.
- Przeprowadź ocenę zagrożenia i ryzyka oraz opracuj pisemne procedury dotyczące powrotu do normalnego — dobrze zdefiniowanego — stanu działania dostosowanego do wyników oceny.
- Rozważ planowanie awaryjne poprzedzone analizą różnego rodzaju ryzyka i cele ataków. Zdefiniuj plany awaryjne i przetestuj je, wykonując ćwiczenia. Regularnie przeglądaj plany awaryjne i odpowiednio je dostosowuj.
- W planach ciągłości działania i naprawy uwzględnij aspekty współpracy z innymi podmiotami.
- Zdefiniuj ważne parametry ciągłości biznesowej firmy, takie jak docelowy czas przywracania funkcjonowania systemu RTO (ang. *Recovery Time Objective*), cel punktu przywracania RPO (ang. *Recovery Point Objective*), maksymalny dopuszczalny przestój MTO (ang. *Maximum Tolerable Outage*) i minimalny cel ciągłości biznesowej MBCO (ang. *Minimum Business Continuity Objective*).

Dodatkowe wskazówki i komentarz:

Wprowadzenie rozwiązań uwierzytelnienia między urządzeniami ma na celu w szczególności ochronę przed nieuprawnioną ponowną kalibracją lub rekonfiguracją, np. urządzeń pomiarowych, poprzez:

- zasadę ograniczonych przywilejów w dostępie do konfiguracji urządzeń i narzędzi kalibracyjnych
- silną autoryzację i uwierzytelnianie personelu posiadającego dostęp do narzędzi inżynierskich
- silne bezpieczeństwo fizyczne dla urządzeń poziomu L0/L1
- wyłączenie podatnych protokołów bezprzewodowych
- wyłączenie funkcji testowania / debugowania

Struktura organizacyjna każdego przedsiębiorstwa jest inna, zatem trudno o uniwersalny schemat, zapewniający kompleksowe podejście do cyberbezpieczeństwa każdej firmie. Prawdopodobnie najważniejsze zasoby i procesy wewnątrz Twojego przedsiębiorstwa są Ci doskonale znane, ale czy orientujesz się, jakie wymagania i zalecenia wynikają z krajowego systemu cyberbezpieczeństwa w Polsce? Aby prawidłowo ocenić kluczowe obszary ochrony oraz swoje słabe punkty, dowiedz się, jakie informacje o cyberbezpieczeńswie zawarte są w międzynarodowych normach oraz krajowych regulacjach prawnych.

2. Utwórz struktury zarządzające bezpieczeństwem cyfrowym swojej firmy

W celu zapewnienia podstawowej ochrony:

- Powołaj osobę lub grupę osób odpowiedzialnych za bezpieczeństwo teleinformatyczne twojej organizacji. Określ najważniejsze cele i podstawowe zadania.
- Wyznacz osobę odpowiedzialną za zapewnienie zgodności prowadzonych działań z zasadami RODO
- Aby zapewnić jak najpełniejsze bezpieczeństwo w skomputeryzowanym ekosystemie, przyjmij podejście całościowe (holistyczne) i opracuj z zespołem architekturę całości zabezpieczeń dostosowaną do ryzyka w oparciu o wymagania biznesowe i charakterystykę działalności firmy.
- Wprowadź ścisłą współpracę między działem OT i IT (a w przypadku sieci IoT utwórz jeden dział informatyczny zajmujący się osobno cyberbezpieczeństwem). Nie zezwalaj osobom odpowiedzialnym za bezpieczeństwo IT na wdrażanie jakichkolwiek polityk cyberbezpieczeństwa, w tym zarządzania podatnościami, po stronie OT bez pełnej wiedzy i współpracy obu działów. Upewnij się, że działy IT i OT dzielą się swoją wiedzą o działaniu systemów, oraz zagrożeniach dla nich.

W celu zapewnienia zaawansowanej ochrony:

- Określ, czy zakres twojej działalności generuje obowiązek powołania Inspektora Ochrony Danych Osobowych (IODO). Wyznacz zakres jego obowiązków oraz zapewnij mu niezależność.
- Sprawdź, czy stosowane metody ochrony danych są wystarczające za pomocą audytu zgodności z RODO — wybierz dogodny sposób przeprowadzenia audytu
- Wprowadź we wszystkich działaniach podejście „privacy by design", którego istotą jest to, by środki bezpieczeństwa związane z prywatnością i ochroną danych były integralną częścią kultury organizacyjnej i wszystkich systemów firmowych.
- Wprowadź środki bezpieczeństwa prywatności i danych poprzez:
  - określenie zakresu danych, które będą przetwarzane przez urządzenia lub systemy w firmie oraz cel tego przetwarzania, w oparciu o obowiązujące przepisy lokalne i międzynarodowe (m.in. RODO), unikając gromadzenia lub niepotrzebnego podawania danych wrażliwych.
  - ustalenie fizycznej lokalizacji przechowywania danych i określ, między którymi działami będą przekazywane dane, ograniczając dostęp do zebranych danych osobowych tylko do upoważnionych osób.
  - przeprowadzenie analizy wpływu na prywatność PIA (ang. *Privacy Impact Assessment*) dla danych, które będą przetwarzane przez urządzenia i systemy firmowe.
  - oddzielenie danych, które mogą posłużyć do identyfikacji osób od innych informacji i zapewnienia ich bezpieczeństwa, np. poprzez szyfrowanie wszelkich danych osobowych przesyłanych w środowisku Przemysłowego Internetu Rzeczy IIoT (ang. *Industrial Internet of Things*).

Dodatkowe wskazówki i komentarz:

Ze względu na fakt, iż zagrożenia bezpieczeństwa stają się coraz bardziej powszechne, coraz większa liczba przedsiębiorstw decyduje się na współpracę z dostawcami zarządzanych usług bezpieczeństwa w celu uzupełnienia realizowanych działań w zakresie bezpieczeństwa wewnętrznego swojej firmy. Dostawcy zarządzanych usług bezpieczeństwa są podmiotami zewnętrznymi, które zarządzają oraz wdrażają rozwiązania w zakresie bezpieczeństwa sieci oraz inne formy ochrony organizacji. Ich usługi mogą obejmować: zapewnienie ochrony przed wirusami i spamem, konfigurację firewalla, wykrywanie prób włamań, zabezpieczanie wirtualnych sieci prywatnych VPN (ang. *Virtual Private Network*), modernizację systemów organizacji wewnątrz firmy. Większość z nich świadczy również różnego rodzaju usługi doradcze w zakresie zapewnienia cyberbezpieczeństwa.

Przykład dobrych praktyk musi iść „ z góry” ale musi być oparty na wiedzy na temat potrzeb i funkcjonowania organizacji pochodzący „z dołu”.

Wprowadź procesy zarządzania ryzykiem przyjmując jednocześnie dwa różne podejścia:

- Odgórne, aby zastosować podejście holistyczne z dobrze zdefiniowaną strategią dotyczącą sposobu rozwiązywania problemów związanych z bezpieczeństwem organizacji z uwzględnieniem jej potrzeb biznesowych. Pomoże to zająć się cyberbezpieczeństwem z perspektywy całej organizacji poprzez jednolite zasady, procedury i praktyki.
- Oddolne, aby zapewnić bardzo szczegółowy obraz sytuacji firmy, również z perspektywy ludzi i systemów informatycznych. Pozwoli to na wyodrębnienie różnic pomiędzy działami, rolami personelu, określonymi procesami itp. Pozwoli to dostosować program wprowadzania cyberbezpieczeństwa całej organizacji do konkretnych potrzeb, również dla mniejszych części organizacji. Połącz te dwa podejścia, aby ustanowić plan bezpieczeństwa dostosowany do całej organizacji i jej konkretnych aspektów również dla najniższego poziomu.

3. Opracuj politykę bezpieczeństwa swojej firmy

W celu zapewnienia podstawowej ochrony:

- Określ zadania i zakres odpowiedzialności pracowników różnych szczebli w zakresie zapewnienia bezpieczeństwa cyfrowego, w tym osób odpowiedzialnych za cyberbezpieczeństwo
- Opracuj regulamin korzystania z technologii teleinformatycznych przez pracowników w postaci spisanego dokumentu, będącego obowiązującą polityką bezpieczeństwa twojej firmy
- Upewnij się, iż polityka bezpieczeństwa jest dokumentem zrozumiałym i spójnym
- Opracuj procedury przyjmowania i odejścia pracowników i stażystów
- Bądź na bieżąco ze zmianami w zakresie bezpieczeństwa cyfrowego i aktualizuj informacje i wytyczne dla pracowników na podstawie wiedzy i doświadczeń

W celu zapewnienia zaawansowanej ochrony:

- Opracuj plan szkoleń pracowników w zakresie cyberbezpieczeństwa
- Zadbaj, aby poza polityką bezpieczeństwa, powstały oddzielne dokumenty, zawierające szczegółowe zasady zabezpieczeń, instrukcje reagowania na incydenty bezpieczeństwa, opisy właściwego sposobu korzystania z danych bądź przydzielania uprawnień dostępu użytkownikom.
- Przygotuj spersonalizowany zbiór Procedur Nadzoru Cyberbezpieczeństwa (PNC), który będzie chronił przed skutkami cyberataków. Dokładne i solidne podręczniki Procedur Nadzoru Cyberbezpieczeństwa są podstawą każdego dobrego programu zgodności z przepisami i wymaganiami branżowymi.
- Wprowadź we wszystkich działaniach podejście „security by design, które należy stosować między innymi przy projektowaniu całego systemu informatycznego.
- Przeprowadź analizę ryzyka i zagrożeń z udziałem ekspertów ds. cyberbezpieczeństwa już na bardzo wczesnym etapie procesu projektowania i budowania systemu informatycznego w firmie, aby dowiedzieć się, jakie funkcje bezpieczeństwa będą niezbędne.

Dodatkowe wskazówki i komentarz:

Polityka bezpieczeństwa powinna:

- być przygotowana odrębnie dla każdego przedsiębiorstwa. Kupowanie wzorów polityki bezpieczeństwa w celu ich skopiowania jest działaniem pozbawionym sensu.
- stanowić wsparcie w realizacji misji przedsiębiorstwa, a nie utrudnienie procedur
- nawiązywać do obowiązujących firmę aktów prawnych oraz uznanych norm i standardów
- uwzględniać trzy wymiary bezpieczeństwa — bezpieczeństwo osobowe (personalne), fizyczne oraz techniczne (w tym cyberbezpieczeństwo)
- uwzględniać zewnętrzne i wewnętrzne uwarunkowania, które mają wpływ na jej skuteczność
- opierać się na rzetelnej ocenie rzeczywistości i analizie ryzyka
- być przygotowana przez osoby, które dysponują wiedzą specjalistyczną zakresie IT, ale również znają firmę lub branżę, w której ona funkcjonuje.

Procedury Nadzoru Cyberbezpieczeństwa (PNC) to fundamentalny element kultury cyberbezpieczeństwa. Pozwolą organizacji jasno zidentyfikować normy, praktyki i oczekiwane zachowania w zakresie cyberbezpieczeństwa, które mają wpływać na to, jak pracownicy podejmują i realizują decyzje w trakcie realizacji programu cyberbezpieczeństwa dla firmy. Rozsądnie opracowane PNC powinny być proste, nieskomplikowane i zazwyczaj odnoszą się do „kto", „co" i „kiedy"powinien zrobić w sytuacjach zagrożenia cybernetycznego. Powinny być one zgodne z dokumentem i / lub procedurami i polityką cyberbezpieczeństwa firmy. PNC pozwolą 1) zapewnić kontrolę regulacyjną w zakresie cyberbezpieczeństwa; 2) zapewnić organizacji i jej pracownikom mapę drogową do poruszania się po przepisach i obowiązkach wynikających z regulacji; 3) określić minimalne mechanizmy kontroli cyberbezpieczeństwa; 4) upoważnić do nadzorowania działań związanych z dostępem do systemu uprzywilejowanych użytkowników.

4. Zadbaj o aktualną wersję oprogramowania na firmowych urządzeniach

W celu zapewnienia podstawowej ochrony:

- Zaktualizuj oprogramowanie na wszystkich stacjach roboczych, systemach i urządzeniach mobilnych najszybciej, jak to możliwe.
- Upewnij się, że administrator systemu jest świadomy odpowiedzialności za aktualizację systemu na bieżąco, bez zbędnej zwłoki.
- Zorganizuj schemat automatycznego aktualizowania oprogramowania i cyklicznie sprawdzaj, czy jest on skuteczny.

W celu zapewnienia zaawansowanej ochrony:

- Monitoruj swoich podwykonawców i firmy zewnętrzne które prowadzą prace lokalne lub zdalne na Twojej infrastrukturze technicznej poprzez wdrożenie odpowiednich zabezpieczeń np. w postaci wdrożenia systemu rejestracji sesji zdalnych co zapewni możliwość ich rozliczenia z wykonanych prac.
- Wprowadź system uwierzytelnienia i autoryzacji wszystkich urządzeń IIoT w sieci, korzystając z odpowiednich i najlepszych dostępnych metod.
- Zdefiniuj kanały wymiany danych między urządzeniami IIoT w postaci „białej listy" i jeśli to możliwe stosuj tylko wybrane bezpieczne kanały.
- Zdefiniuj i zaimplementuj także „białe listy" aplikacji i aktualizuj je przynajmniej raz w roku oraz w przypadku dokonywania zmian w systemie.
- Zapewnij integralność danych pochodzących z systemów produkcyjnych poprzez zastosowanie odpowiednich mechanizmów kryptograficznych oraz systemu przechowywania kluczy dostosowanego do możliwości wdrożonych rozwiązań.
- Monitoruj dane pochodzące z systemów produkcyjnych w stanie spoczynku (*at rest*) i podczas transferu (*in transit*), aby zidentyfikować potencjalną nieautoryzowaną modyfikację danych.
- Wdrażaj uaktualnienia i „patche" oprogramowania i systemów operacyjnych dla systemów IIoT dopiero po ustaleniu, że nie spowodują one żadnych negatywnych konsekwencji oraz przetestuj „patche" w środowisku testowym przed wdrożeniem ich w systemach produkcyjnych.
- Weryfikuj autentyczność i integralność oprogramowania również dla urządzeń końcowych i zapewnij ścisłą oraz regularną kontrolę odpowiedniego personelu nad ich aktualizacją.
- Zezwalaj stronom trzecim na wykonywanie poprawek w systemach i oprogramowaniu tylko wtedy, gdy gwarantują i są w stanie udowodnić, że „patch" został przetestowany i nie spowoduje żadnych negatywnych konsekwencji dla urządzenia lub systemu albo jeśli strona trzecia przyjmie pełną odpowiedzialność za aktualizację zgodnie z obowiązującą umową.
- Zweryfikuj źródła aktualizacji oprogramowania i wykonywania automatycznych procedur aktualizacji oprogramowania tylko wtedy, gdy są one oparte na analizie ryzyka.
- Zezwalaj stronom trzecim na wykonywanie poprawek tylko wtedy, gdy gwarantują i są w stanie udowodnić, że łatka została przetestowana i nie spowoduje żadnych negatywnych konsekwencji na urządzeniu lub jeśli przyjmą odpowiedzialność za aktualizację zgodnie z obowiązującą umową.

Dodatkowe wskazówki i komentarz:

Obecnie wszyscy producenci systemów IT/OT zapewniają dostęp do aktualizacji bezpieczeństwa w zakresie oferowanych przez siebie produktów. Należy zwrócić uwagę, iż zdecydowana większość cyberataków wynika z wykorzystania przez hakerów podatności systemów, które zostały wcześniej udokumentowane, a producenci opublikowali naprawiające je poprawki. Warto pamiętać, iż systematyczne instalowanie aktualizacji bezpieczeństwa jest podstawą, bez której żadne inne środki bezpieczeństwa nie mogą stać się skuteczne. Jeśli nie potrafisz zaktualizować systemu w ramach jakiegoś urządzenia, po prostu zastanów się nad jego wymianą na inny, nowszy, bezpieczniejszy model.

5. Zapewnij skuteczną ochronę antywirusową

W celu zapewnienia podstawowej ochrony:

- Upewnij się, że oprogramowanie antywirusowe jest zainstalowane na wszystkich stacjach roboczych i serwerach
- Sprawdź, czy program antywirusowy jest automatycznie aktualizowany i zgodny z najnowszą rekomendowaną wersją
- Utwórz schemat postępowania pracownika w przypadku otrzymania ostrzeżenia o niebezpiecznych plikach lub wiadomości o wykryciu wirusa lub zagrożenia

W celu zapewnienia zaawansowanej ochrony:

- Zleć administratorowi wykonanie bieżących analiz i rejestru występujących zagrożeń i incydentów
- Zadbaj o to, by również urządzenia mobilne (telefony, tablety) miały wgrany sprawny i aktualny program antywirusowy
- Rozważ stosowanie systemu anti-malware

Dodatkowe wskazówki i komentarz:

Na rynku jest dostępnych wiele produktów antywirusowych, dedykowanych dla przedsiębiorców. Warto zapoznać się z aktualnymi zestawieniami i rankingami, dotyczącymi testowania tego typu produktów. Zdecydowanie należy unikać korzystania z programów o najniższej reputacji i nie zalecane przez organizacje rządowe typu MON, ABW. Może okazać się, że są to produkty o ograniczonej funkcjonalności lub że nie dysponują one odpowiednią, często aktualizowaną bazą sygnatur i mogą być one szkodliwe dla organizacji.

6. Zabezpiecz sieć firmową za pomocą firewalla

W celu zapewnienia podstawowej ochrony:

- Dokonaj zakupu i wdrożenia systemu bezpieczeństwa typu firewall
- Zleć profesjonalistom konfigurację zapór sieciowych

W celu zapewnienia zaawansowanej ochrony:

- Zleć administratorowi analizę rejestru alertów i incydentów związanych z zaporą sieciową
- Zweryfikuj skuteczność stosowanej zapory sieciowej za pomocą cyklicznych audytów, celem weryfikacji wdrożonych reguł filtrujących

Dodatkowe wskazówki i komentarz:

Podstawowym celem konfiguracji firewalla jest wdrożenie procedury automatycznego skanowania każdego przychodzącego i wychodzącego pakietu danych oraz sprawdzenie złośliwej lub nieodpowiedniej zawartości, a następnie zezwalanie lub blokowanie wprowadzenia pakietu danych do systemu firmy. Od pewnego czasu na rynku istnieją zapory sieciowe nowej generacji — NGFW (ang. Next Generation Firewall). Mogą one być oparte bądź na oprogramowaniu bądź sprzęcie i mogą posunąć się dalej niż zwykła ocena pakietów danych. Z ich pomocą możliwa jest głęboka inspekcja pakietów, bez ograniczania się tylko do sprawdzenia numerów portów i typów protokołów. Umożliwiają one kontrolę ruchu na poziomie warstwy aplikacji, zapobiegają włamaniom i mogą korzystać z różnych mechanizmów wykraczających poza funkcjonalność klasycznej zapory sieciowej.

7. Utwórz bezpieczny system zdalnego dostępu

W celu zapewnienia podstawowej ochrony:

- Każdy zdalny dostęp do sieci firmowej powinien odbywać się za pośrednictwem szyfrowanego połączenia i przy użyciu dwóch czynników uwierzytelnienia 2FA (ang. *Two-Factor Authentication*)
- Utwórz indywidualne konta dla każdego użytkownika
- Wprowadź uwierzytelnianie wieloskładnikowe w systemach IIoT
- Zmień domyślne hasła i nazwy użytkownika podczas uruchamiania / pierwszego użycia urządzenia, oprogramowania bądź systemu. Staraj się używać systemów bezhasłowych.
- Opracuj zestaw reguł kontroli zdalnej komunikacji
- Ogranicz możliwość zdalnego dostępu do sytuacji, w których jest on konieczny i niezbędny dla prowadzenia działalności
- Wprowadź zasadę, że po określonym okresie bezczynności zdalne połączenie także z urządzeniami IIoT powinno zostać automatycznie rozłączone i wymagane jest kolejne uwierzytelnienie użytkownika za pomocą loginu, hasła, tokenu itp.

W celu zapewnienia zaawansowanej ochrony:

- Zaszyfruj połączenia i zapewnij prywatność firmie poprzez wykorzystanie połączeń VPN celem dostania się do zasobów wewnętrznych firmy.
- Zastosuj dodatkowe, wzmocnione metody autentykacji połączeń z zewnętrznych sieci publicznych
- Wprowadź ograniczenia zdalnego dostępu dla wybranych lokalizacji geograficznych, wyznaczając możliwość uzyskania dostępu tylko wybranym adresom IP lub lokalizacji.
- Zastosuj zasadę najmniejszej ilości uprawnień i upewnij się, że w środowisku z wieloma użytkownikami role są odpowiednio rozdzielone i zatwierdzone przez odpowiednią osobę.
- Zapewnij poziom najmniejszej możliwej ilości uprawnień dotyczących uwierzytelnienia urządzeń i systemów IIoT oraz upewnij się, że uwierzytelnienie umożliwia dostęp tylko do określonego segmentu systemu.
- Zastosuj rozwiązanie typu zarządzanie dostępem uprzywilejowanym PAM (ang. *Privilege Access Management*) w przypadku rozległych i zróżnicowanych sieci z dużą liczbą urządzeń.
- Rozważ w ramach kontroli dostępu także aspekty fizycznego dostępu do budynków, obszarów, pomieszczeń i szaf

Dodatkowe wskazówki i komentarz:

Będąc poza biurem, pamiętaj aby nie korzystać z otwartych sieci Wi-FI. Ogólnodostępne sieci, z których można skorzystać w centrach handlowych, bibliotekach, hotelach czy restauracjach, nie są najczęściej odpowiednio chronione. Przejęcie kontroli nad taką siecią nie jest zadaniem trudnym dla cyberprzestępców. Korzystanie z Internetu za pośrednictwem publicznego Wi-Fi może się okazać pozorną oszczędnością. Najlepszą i najbezpieczniejszą alternatywą dla publicznych sieci Wi-Fi jest korzystanie z własnej sieci komórkowej.

8. Chroń zasoby cyfrowe firmy

W celu zapewnienia podstawowej ochrony:

- Wybierz odpowiednie dla swojej działalności rozwiązanie w zakresie procesu tworzenia kopii zapasowych
- Zleć administratorowi lub zespołowi IT wdrożenie wykonywania kopii zapasowych kluczowych danych firmy oraz danych które są cenne z punktu widzenia biznesowego.
- Rozważ opcję przechowywania danych w chmurze internetowej
- Przetestuj wybrany system tworzenia kopii zapasowych, aby upewnić się, że działa on prawidłowo i kopie zapasowe można odtworzyć w dowolnym momencie
- Przechowuj kopie zapasowe w bezpiecznym miejscu, które jest odpowiednio zabezpieczone przed dostępem niepowołanych osób.

W celu zapewnienia zaawansowanej ochrony:

- Przechowuj dane w ramach centrum przetwarzania danych dla podniesienia poziomu ich bezpieczeństwa
- Użyj dodatkowych metod szyfrowania dostępu do danych, przechowywanych w chmurze (poza standardowymi środkami bezpieczeństwa, oferowanymi przez usługodawcę)
- Zapewnij zabezpieczenie danych w spoczynku (*at rest*), podczas przesyłania (*in transit*) i użytkowania (*in use*) we wszystkich rodzajach pamięci.
- Wprowadź szyfrowanie i zarządzanie kluczami w przypadku danych o wysokim stopniu poufności, tak aby informacje mogły być odczytane tylko przez upoważnionych użytkowników oraz stosowanie rozwiązań zapobiegających utracie danych.
- Wprowadź anonimizację i zabezpieczenie wszelkich bezpośrednich lub pośrednich danych osobowych przetwarzanych w firmie, np. poprzez kontrolę dostępu opartą na rolach oraz szyfrowanie z uwzględnieniem wszystkich wymogów prawnych.

Dodatkowe wskazówki i komentarz:

Kopie zapasowe najważniejszych danych powinny być wykonywane regularnie, na odrębnym nośniku danych (przykładowo: dysk USB, macierze dyskowe) lub na dyskach wirtualnych (chmury obliczeniowe, takie jak Google Drive, Microsoft OneDrive, Amazon Drive). W zasadzie nie powinno się też posiadać tylko jednego zestawu kopii bezpieczeństwa.

9. Zabezpiecz komponenty systemu w chmurze

W celu zapewnienia podstawowej ochrony:

- Wprowadź adekwatne środki bezpieczeństwa dotyczące różnych aspektów bezpieczeństwa przetwarzania w chmurze.
- Opieraj swoje decyzje dotyczące wyboru typu chmury na ocenie wpływu na biznes i prywatność, biorąc również pod uwagę przepisy prawa i regulacje mające zastosowanie do kraju i punktów obecności dostawcy usług w chmurze.
- Uwzględnij aspekty bezpieczeństwa i dostępności w umowach z dostawcami zabezpieczeń chmury.
- Unikaj, w przypadku aplikacji i systemów opartych na chmurze oraz w przypadku systemów scentralizowanych, słabych punktów które mogą stać się przyczyną awarii jego całości — np. jednego słabego punktu dostępu albo niezabezpieczonego urządzenia, przez które cyberprzestępcy mogą przejąć kontrolę nad całością.

W celu zapewnienia zaawansowanej ochrony:

- Zdefiniuj krytyczne systemy i aplikacje w prywatnych lub przynajmniej hybrydowych modelach wdrażania i poprzedzaj wdrożenie analizą ryzyka, jeśli rozważasz zastosowanie chmury publicznej.
- Zastosuj podejście do bezpieczeństwa opartego na zasadzie „zero-knowledge" i chroń wszystkie dane w chmurze i podczas transferu do niej, aby zmniejszyć ryzyko związane z atakami w chmurze.

10. Zapewnij bezpieczeństwo na linii Maszyna-Maszyna M2M (ang. *Man to Machine*)

W celu zapewnienia podstawowej ochrony:

- Wprowadź środki bezpieczeństwa dotyczące przechowywania kluczy, szyfrowania, sprawdzania poprawności danych wejściowych i ochrony w zakresie bezpieczeństwa w komunikacji na linii Maszyna-Maszyna.
- Wykorzystuj bezpieczne, lekkie i wydajne algorytmy szyfrowania między komunikującymi się urządzeniami, aby zapewnić też ich wzajemne uwierzytelnianie oraz integralność i poufność przekazywanych między nimi danych.

W celu zapewnienia zaawansowanej ochrony:

- Używaj protokołów komunikacyjnych, które zawierają funkcję wykrywania, czy całość lub część wiadomości jest nieautoryzowanym powtórzeniem wcześniejszej wiadomości.
- Przechowuj klucze służące do szyfrowania komunikacji (inne niż klucze publiczne) na serwerze HSM (ang. Hardware Security Module) znajdującym się w sprzęcie infrastruktury lub jeśli używasz odpowiednio bezpiecznych rozwiązań chmurowych to na serwerze HSM w chmurze.

11. Wprowadź zarządzanie integralnością oraz wiarygodnością danych i urządzeń

W celu zapewnienia podstawowej ochrony:

- Sprawdź integralność oprogramowania przed rozpoczęciem jego uruchamiania, upewniając się, że pochodzi ono z wiarygodnego źródła i zostało pozyskane w bezpieczny sposób.
- Wprowadź rozwiązania zapewniające bezpieczeństwo oraz integralność danych produkcyjnych poprzez zastosowanie odpowiednich, wydajnych mechanizmów kryptograficznych, które mogą być obsługiwane przez wszystkie urządzenia, tak aby bezpieczeństwo danych między możliwie wszystkimi urządzeniami.

W celu zapewnienia zaawansowanej ochrony:

- Monitoruj dane produkcyjne w stanie spoczynku (*at rest*) i podczas ich przekazywania (*in transit*), aby zidentyfikować potencjalną nieautoryzowaną modyfikację danych.
- Wprowadź rozwiązania umożliwiające uwierzytelnienie wszystkich urządzeń IIoT w sieci między sobą z wykorzystaniem odpowiednio silnych i bezpiecznych metod, które zapewnią bezpieczeństwo nie tylko obecnie oraz nie będą zagrożone atakami z wykorzystaniem komputerów kwantowych (np. infrastruktura klucza publicznego PKI — ang. *Public Key Infrastructure*)

12. Zabezpiecz serwery i komponenty sieciowe

W celu zapewnienia podstawowej ochrony:

- Ustal narzędzia kontroli dostępu do serwerów (różne narzędzia charakteryzują się różnym stopniem skuteczności — od haseł po czytniki linii papilarnych, karty lub kody dostępu)
- Cyklicznie zmieniaj hasła dostępu do serwerów
- Zapewnij zasilanie awaryjne
- Upewnij się, że posiadasz odpowiedni system przeciwpożarowy
- Rozważ możliwość korzystania z serwerów na zasadzie najmu
- Zablokuj możliwość zdalnego dostępu do serwera bezpośrednio z Internetu, stosuj stacje przesiadkowe
- Odseparuj sieć firmową od sieci Wi-Fi dla gości

Dla zapewnienia zaawansowanej ochrony:

- Zapewnij nieprzerwaną pracę serwerów, dzięki klastrom wysokiej dostępności HA (ang. *High Availability*)
- Dokonuj cyklicznej aktualizacji serwera, tworząc wcześniej kopie zapasowe danych.
- Chroń firmową sieć Wi-Fi- za pomocą najnowszego pakietu zabezpieczeń
- Korzystaj z systemów wykrywania IDS (ang. *Intrusion Detection System*) i zapobiegania włamaniom i IPS (ang. I*ntrusion Prevention System*)
- Ogranicz fizyczny dostęp do pomieszczeń, w których znajdują się serwery i urządzenia sieciowe
- Zapewnij weryfikację zabezpieczeń za pomocą testów penetracyjnych i audytów.

Dodatkowe wskazówki i komentarz:

Testy penetracyjne to kontrolowane próby przełamania zabezpieczeń systemu informatycznego, które symulują ataki hakerów. Ich celem jest sprawdzenie, czy istnieje w systemie podatność, umożliwiająca pokonanie zabezpieczeń, włamanie się lub przejęcia kontroli nad systemem. Testy penetracyjne mogą być wykonywane z sieci Internet (testy zewnętrzne) lub z sieci firmowej LAN (testy wewnętrzne). Audytorzy wykorzystują własną oraz udostępnioną im wiedzę do przełamywania kolejnych zabezpieczeń. Testy penetracyjne najwierniej odzwierciedlają realne próby włamań.

13. Opracuj zasady używania haseł oraz uprawnienia dostępu do zasobów

W celu zapewnienia podstawowej ochrony:

- Zawsze zmieniaj domyślne hasła, które zostały wybrane w sposób automatyczny, na takie które jest jak najbardziej złożone i możliwie długie
- Aktualizuj na bieżąco listę aktywnych kont użytkowników
- Określ zasady tworzenia haseł dla użytkowników, z odpowiednią liczbą i rodzajem użytych znaków (przykładowo: minimum 10 znaków, zawierających przynajmniej dwie cyfry lub znaki oraz wielkie i małe litery)
- Bezzwłocznie dezaktywuj konta użytkowników, które już nie będą używane np. w momencie odejścia, zwolnienia pracownika
- Uświadom pracowników, aby zawsze korzystali z własnych kont oraz nie udostępniali sobie wzajemnie haseł (nie umieszczali ich w widocznym miejscu przy stacji roboczej, nie wysyłali ich za pomocą telefonów komórkowych lub poczty mailowej)
- Korzystaj z zaawansowanych metod uwierzytelniania (np. metod bezhasłowych)
- Zadbaj, by uprawnienia dostępu do zasobów nadawane były pod kontrolą administratora.

W celu zapewnienia zaawansowanej ochrony:

- Poproś administratora systemu o ocenę zasadności bieżących uprawnień dostępu do zasobów w przypadku każdego pracownika.
- Skonfiguruj zaawansowany system dostępu do zasobów, w którym użytkownicy mają dostęp tylko do tych elementów systemu, które są im niezbędne lub potrzebne w trakcie wykonywania swoich obowiązków
- Zleć sprawdzenie przypadków nietypowych aktywności użytkowników w zakresie dostępu do zasobów systemu, rejestruj wszystkie logowania.

Dodatkowe wskazówki i komentarz:

Uwierzytelnianie dwuskładnikowe (2FA — ang. *Two Factor Authentication*) zapewnia nieporównywalnie wyższy poziom bezpieczeństwa niż klasyczne, nawet bardzo silne hasło. Mechanizm ten polega na wykorzystaniu w procedurze logowania nie tylko indywidualnego hasła, ale również urządzenia mobilnego lub danych biometrycznych (skan odcisku palca lub tęczówki oka). Mechanizm ten najczęściej polega na wykorzystaniu specjalnego kodu, generowanego przez token kryptograficzny, którym w większości przypadków jest dedykowana aplikacja zainstalowana na telefonie komórkowym.

14. Chroń dane osobowe pracowników i klientów firmy

W celu zapewnienia podstawowej ochrony:

- Określ, jakie dane osobowe gromadzisz i przetwarzasz, jaki jest cel ich gromadzenia oraz podstawa prawna
- Przechowuj tylko konieczne dane osobowe i tylko do momentu, kiedy są one potrzebne
- Zaszyfruj dostęp do nośników, na których przechowujesz dane osobowe
- Poproś o utworzenie dokumentacji, dotyczącej sposobu i celu przetwarzania danych osobowych w twojej firmie

W celu zapewnienia zaawansowanej ochrony:

- Przeprowadź ocenę skutków wycieku danych lub niewłaściwego wykorzystywania posiadanych danych osobowych
- W przypadku niektórych rodzajów działalności, konieczne może być powołanie inspektora ochrony danych osobowych
- Jeśli prowadzisz witrynę e-commerce lub w inny sposób przetwarzasz płatności za pośrednictwem swojej witryny internetowej, upewnij się, że dostawca danego serwisu internetowego posiada odpowiednie zabezpieczenia, szyfrujące dane klientów (imię, nazwisko, dane karty kredytowej) podczas ich przesyłania.

Dodatkowe wskazówki i komentarz:

RODO nakłada szereg obowiązków na przedsiębiorców, prowadzących swoją działalność gospodarczą na terenie Unii Europejskiej. Zgodnie z przepisami rozporządzenia, każdy administrator danych ma obowiązek informowania organu nadzorczego o naruszeniu ochrony danych osobowych, jeśli zdarzenie to mogło skutkować trafieniem prywatnych informacji w niepowołane ręce. Każde przedsiębiorstwo jest również zobowiązane do prowadzenia rejestru przetwarzania danych osobowych, który zawiera informacje o: rodzaju danych, celu i sposobu ich przetwarzania oraz informacji o tym, przez kogo są one przetwarzane.

15. Zabezpiecz stacje robocze oraz mobilne urządzenia

W celu zapewnienia podstawowej ochrony:

- Upewnij się, że system jest automatycznie blokowany po określonym czasie braku aktywności
- Wymagaj od pracowników, aby blokowali dostęp do systemu podczas każdej, nawet krótkiej nieobecności przy stacji roboczej
- Zwróć uwagę na politykę czystego biurka oraz zapewnij, iż istnieje nadzór nad ekipą sprzątającą biuro
- Nigdy nie zostawiaj firmowych urządzeń mobilnych poza zasięgiem wzroku lub w miejscach, które są one narażone na kradzież (np. samochód, pokój hotelowy)

W celu zapewnienia zaawansowanej ochrony:

- Upewnij się, że likwidowane nośniki danych, dokumenty i zasoby drukowane są niszczone w sposób, uniemożliwiający odczyt zawartych w nich danych.
- Wprowadź zakaz używania własnych urządzeń (w szczególności pendrive'ów, kart pamięci i dysków zewnętrznych) przez pracowników w obrębie firmy oraz łączenia ich z siecią firmową
- Zapewnij szyfrowanie dysków na przenośnych komputerach
- Zadbaj o dodatkowe zabezpieczenia, w przypadku kopiowania danych szczególnie wrażliwych i kluczowych dla firmy

Dodatkowe wskazówki i komentarz:

Jeśli nie używasz często kamery, wyłącz ją na stałe za pomocą Menadżera Urządzeń zawartego w Windows 10 i Windows 7. W ten sposób automatycznie wyłączysz także mikrofon oraz możliwość podglądania i podsłuchiwania twoich działań służbowych. Możesz także zwyczajnie zakleić obiektyw kamery za pomocą nieprzezroczystej taśmy.

16. Zabezpiecz sieci i protokoły komunikacji oraz wprowadź ich szyfrowanie

W celu zapewnienia podstawowej ochrony:

- Zapewnij odpowiednią implementację protokołów, szyfrowanie i segmentację sieci by pomóc zapewnić jak najpełniejsze bezpieczeństwo komunikacji.
- Nie lekceważ informacji o podatności protokołów nawet jeśli są znane i szeroko stosowane.
- Wprowadź bezpieczne kanały komunikacji w systemach IIoT oraz szyfrowanie komunikacji między urządzeniami — także tymi o niewielkiej mocy obliczeniowej, o ograniczonej pamięci oraz dostępie do energii, gdyż one mogą stać się najsłabszymi elementami całej sieci.
- Postępuj zgodnie z podejściem „mikro segmentacji", tj. buduj małe wyspy komponentów w ramach jednej sieci, które komunikują się tylko ze sobą i kontrolują ruch sieciowy między segmentami ale zadbaj też o bezpieczną komunikację między tymi wyspami.
- Zapewnij możliwości bezpiecznego współdziałania między protokołami podczas implementacji różnych protokołów dla różnych urządzeń w tym samym systemie. Unikaj protokołów o znanych podatnościach.

W celu zapewnienia zaawansowanej ochrony:

- Ogranicz, jeśli to możliwe, liczbę protokołów zaimplementowanych w danym środowisku skupiając się na protokołach najbardziej bezpiecznych, z najmniejszą liczbą znanych podatności i wyłącz domyślne usługi sieciowe oraz protokoły, które nie są używane.
- Zapewnij właściwe i silne algorytmy szyfrowania wykorzystujące silny i dobrze zaprojektowany system dystrybucji kluczy. Sprawdź solidność implementacji.
- Zapewnij bezpieczne środowisko do wymiany kluczy i zarządzania kluczami, unikając udostępniania kluczy kryptograficznych na wielu urządzeniach w tradycyjnych systemach.
- Zapewnij właściwe i skuteczne wykorzystanie kryptografii w celu ochrony poufności, autentyczności oraz integralności danych i informacji (w tym komunikatów kontrolnych) podczas ich przesyłania (*in transit*) i w spoczynku (*at rest*).

17. Wprowadź regularny monitoring i audyt

W celu zapewnienia podstawowej ochrony:

- Wdrażaj głównie pasywne rozwiązanie monitorujące w środowiskach IT i OT, aby stworzyć linię bazową ruchu w sieci przemysłowej oraz monitorować anomalie i zgodność z linią bazową.
- Wprowadź stosowanie rozwiązań takich jak dzienniki bezpieczeństwa i analizuj je w czasie rzeczywistym za pomocą specjalnie przeznaczonych do tego narzędzi, np. rozwiązań klasy SIEM (ang. Security Information and Event Management), a najlepiej ramach stworzonego na potrzeby zakładu centrum operacji bezpieczeństwa SOC (ang. Security Operation Center).
- Wykonuj okresowe przeglądy dzienników komunikacji sieciowej, uprawnień kontroli dostępu i konfiguracji zasobów.
- Przeprowadzaj regularnie audyty bezpieczeństwa.

W celu zapewnienia zaawansowanej ochrony:

- Monitoruj dostępność urządzeń IIoT w czasie rzeczywistym, jeśli jest to technicznie wykonalne.

Dodatkowe wskazówki i komentarz:

Audyt musi być przeprowadzony przez niezależną organizację zewnętrzną, która zazwyczaj musi posiadać jakiś rodzaj certyfikacji. Organizacja może mieć zespół audytu wewnętrznego, ale zespół ten powinien działać jako niezależna agencja. Należy podkreślić, że audyt jest tylko pierwszym krokiem w zdiagnozowaniu czy procedury bezpieczeństwa w organizacji są na miejscu i są przestrzegane. Podstawowym elementem prawdziwego i faktycznego bezpieczeństwa organizacji jest zapewnienie, że wnioski z audytu będą przestrzegane, a zalecenia zostaną wdrożone.

18. Zapewnij szkolenia w zakresie cyberbezpieczeństwa swoim pracownikom

W celu zapewnienia podstawowej ochrony:

- Przedstaw i wyjaśnij pracownikom założenia polityki bezpieczeństwa oraz uwzględnij ich uwagi i spostrzeżenia
- Zobliguj pracowników do podpisania polityki bezpieczeństwa
- Okresowo przypominaj o założeniach polityki bezpieczeństwa, informuj pracowników o zarejestrowanych incydentach i opisz właściwy sposób reagowania na zagrożenia
- Okresowo przypominaj pracownikom o zasadach ochrony danych osobowych
- Opracuj i kontroluj przestrzeganie zasad bezpieczeństwa w procedurach uiszczania płatności firmowych

W celu zapewnienia zaawansowanej ochrony:

- Traktuj znajomość zasad bezpieczeństwa jako wymóg i element konieczny ścieżki awansu w firmie
- Okresowo sprawdzaj wiedzę pracowników w zakresie cyberbezpieczeństwa, np. za pomocą krótkich testów wielokrotnego wyboru.
- Przyjmij holistyczne podejście do szkoleń i budowania świadomości bezpieczeństwa wśród pracowników — upewnij się, że obejmuje ono pracowników na wszystkich szczeblach, nowe zagrożenia dla środowiska produkcyjnego przez nowe możliwości Przemysłu 4.0 i jest dostosowane do ról i obowiązków pracowników, a także do różnych poziomów wiedzy uczestników.
- Zapewnij wszystkim użytkownikom rozwiązań IIoT podstawowe informacje o bezpieczeństwie i materiały szkoleniowe, zanim uzyskają uprawnienia dostępu do systemu.
- Zapewnij przeszkolenia kadry korzystającej z urządzeń IIoT w zakresie bezpiecznego użytkowania tych urządzeń, wyjaśniając im technologie wdrożone w celu ochrony urządzeń IIoT i całego inteligentnego ekosystemu kładąc nacisk na interoperacyjność elementów.
- Rozważ możliwość komunikowania się z innymi firmami na poziomie sektorowym, w tym łańcucha dostaw tworząc wspólne programy szkoleniowe lub nawiązując współpracę w celu integracji zabezpieczeń.
- W miarę możliwość zapewnij jak największej grupie pracowników z różnych działów możliwość uczestniczenia w przedsięwzięciach technologicznych i edukacyjnych dotyczących cyberbezpieczeństwa.

Dodatkowe wskazówki i komentarz:

Użytkownicy powinni być poinformowani w szczególności o potrzebie zachowania szczególnej ostrożności przy otwieraniu załączników otrzymywanych w wiadomościach e-mail oraz przy wchodzeniu na strony, do których linki otrzymują w wiadomościach e-mailowych lub SMSach. Znaczna część szkodliwego oprogramowania jest dystrybuowana właśnie w ten sposób. Chociaż dostawcy usług pocztowych oraz operatorzy telekomunikacyjni wdrażają wiele zabezpieczeń, aby tego typu wiadomości były odpowiednio oznakowane i filtrowane, skuteczność tych działań nigdy nie będzie pełna.

19. Opracuj schemat działania na wypadek sytuacji kryzysowych

W celu zapewnienia podstawowej ochrony:

- Opracuj plan zarządzania kryzysowego w przedsiębiorstwie, uwzględniając ryzyko zdarzeń losowych oraz wystąpienia cyberzagrożeń
- Przygotuj plan kontynuacji kluczowych procesów, zapewniających ciągłość działania firmy
- Uświadom pracowników, kogo w pierwszej kolejności informować o zaistniałym incydencie bezpieczeństwa. Wyznacz osobę kontaktową do spraw cyberincydentów i cyberzagrożeń w ramach zespołu IT.
- Zabezpiecz dane odnośnie listy kontaktów biznesowych firmy
- Rejestruj zaistniałe incydenty bezpieczeństwa, dla ciągłego udoskonalania, identyfikacji luk i słabych punktów

W celu zapewnienia zaawansowanej ochrony:

- Dokonuj corocznej weryfikacji aktualności założeń przygotowanych planów działania w kryzysowej sytuacji
- Oceń korzyści z ubezpieczenia od cyberzagrożeń i rozważ dostępne opcje
- Ustanów ścisłą współpracę działów OT i IT, zapewniając, że ich współpraca z właścicielami firm systemów, organami decyzyjnymi i innymi interesariuszami jest również skuteczna.
- Wprowadź podejście do zarządzania ryzykiem przeznaczone dla Przemysłu 4.0 i inteligentnej produkcji (ang. *Smart Manufacturing*) uwzględniające nowe zagrożenia i scenariusze ataków.
- Wprowadź proces zarządzania ryzykiem i zagrożeniami zgodnie z indywidualnymi potrzebami i wymaganiami bezpieczeństwa Twojej firmy.
- Przeprowadzaj przynajmniej raz w roku analizę ryzyka, wobec zmieniających się zagrożeń, która obejmuje zwłaszcza nowe aspekty cyberbezpieczeństwa.
- Zintegruj tę analizę również z innymi procesami w firmie, takimi jak zarządzanie zmianami, obsługa incydentów i zarządzanie podatnościami.
- Rozważ włączenie procesu analizy zagrożeń do podejścia do całości procesu zarządzania zagrożeniami w Twojej firmie, opierając się na różnych źródłach informacji, a także udostępnianie informacji na temat zagrożeń zaufanym partnerom branżowym, takim jak ISAC (ang. *Information Sharing and Analysis Center*) i CERT (ang. *Computer Emergency Response Team*).
- Monitoruj wybrane zagrożenia i określaj ich wpływ na systemy, przeprowadzając analizę ryzyka.
- W procesie zarządzania ryzykiem, zastosuj także tutaj jednocześnie dwa różne, a wspomniane wcześniej, podejścia: „odgórne", odnoszące się do cyberbezpieczeństwa z perspektywy całej organizacji oraz „oddolne", zapewniające bardzo szczegółowy i szczegółowy obraz sytuacji firmy.

Dodatkowe wskazówki i komentarz:

Jeśli w porę udało ci się przejrzeć zamiary przestępcy i udaremnić atak, możesz pomóc także uchronić innych. Upublicznij ostrzeżenie, aby utrudnić pracę przestępcom. Możesz też manipulować atakującym, przekazać fałszywe dane, zbierając materiały dowodowe. Kiedy uznasz, że udało ci się zebrać wystarczającą ilość informacji, możesz postarać się nagłośnić sprawę w portalach branżowych zajmujących się bezpieczeństwem lub zgłosić sprawę organom ścigania.

20. Wprowadź zasady bezpieczeństwa we współpracy z podmiotami zewnętrznymi

W celu zapewnienia podstawowej ochrony:

- Ściśle kontroluj dostęp osób trzecich do warstwy kontrolnej lub produkcyjnej,
- Korzystaj ze specjalnie utworzonych i do tego przeznaczonych kont w rejestrze, z systemów uwierzytelniania wieloskładnikowego i szyfrowania. Udzielaj dostępu do warstwy kontrolnej lub produkcyjnej stronom trzecim tylko w określonym przedziale czasowym, w określonym celu i w najmniej uprzywilejowany sposób. Monitoruj, rejestruj i nadzoruj sesje.
- Jasno zdefiniuj wszystkie istotne aspekty partnerstwa ze stronami trzecimi, szczególny nacisk kładąc na bezpieczeństwo, w odpowiednich umowach i kontraktach (np. umowa o gwarantowanym poziomie usług SLA, ang. *Service Level Agreement* czy umowa o zachowaniu poufności NDA, ang. *Non-disclosure agreement*). Podpisz te umowy i kontrakty przed rozpoczęciem współpracy.

W celu zapewnienia zaawansowanej ochrony:

- Wymagaj od dostawców informacji na temat bezpieczeństwa stosowanych przez nich procesów i ich produktu, np. poprzez przygotowanie kwestionariusza dla dostawców na temat ich wkładu w bezpieczeństwo dostarczanych przez nich towarów oraz ich dobór partnerów (np. podwykonawców).
- Aby zwiększyć świadomość w zakresie wspólnego cyberbezpieczeństwa w obszarach współpracy, rozważ komunikację z innymi firmami na poziomie sektorowym, w tym w łańcuchu dostaw (m.in. komunikację z producentami, dostawcami komponentów, dostawcami oprogramowania, usługodawcami i klientami).

Podsumowanie

Cyberbezpieczeństwa nie wystarczy zbudować, trzeba je stale monitorować i dostosowywać do warunków i otoczenia przedsiębiorstwa. Trendy rynkowe, rozwiązania technologiczne, przepisy prawa, oczekiwania klientów oraz rodzaje przestępczości zmieniają się w bardzo szybkim tempie. Cyberbezpieczeństwem należy zatem zarządzać w sposób systemowy i ciągły, aby nadążyć z jego dostosowaniem do zmieniających się warunków. Priorytetem dla każdego przedsiębiorcy powinno być przede wszystkim przestrzeganie regulacji prawnych obowiązujących w zakresie cyberbezpieczeństwa oraz opracowanie własnej polityki bezpieczeństwa, dostosowanej do specyfiki firmy.