



CYBERBEZPIECZEŃSTWO W ZINFORMATYZOWANYM ŚRODOWISKU PRACY

Człowiek + Maszyna = Niebezpieczna relacja? / Bezpieczeństwo pracy zależy od Ciebie



1

Cyberbezpieczeństwo w z informatyzowanym środowisku pracy

Zinformatyzowane środowisko pracy



2

Cyberbezpieczeństwo w z informatyzowanym środowisku pracy

Cyberprzestrzeń

Cyberprzestrzeń to interaktywna domena stworzona z cyfrowych sieci, która jest wykorzystywana do przechowywania, modyfikowania oraz przekazywania informacji. Jej częścią jest Internet, ale zawierają się w niej także inne systemy informacyjne, które obsługują nasz biznes, infrastrukturę oraz wspomagają świadczenie usług.

Cyberprzestrzeń jest wirtualną przestrzenią wszystkich systemów technologii informacyjnej powiązanych na poziomie danych w skali globalnej. Fundament cyberprzestrzeni stanowi Internet jako uniwersalna oraz powszechnie dostępna sieć oferująca połączenia oraz transport, która może być uzupełniania oraz rozszerzana dalej przez dowolną ilość dodatkowych sieci danych. Systemy IT działające w wyizolowanej przestrzeni wirtualnej nie stanowią części cyberprzestrzeni.

Cyberprzestrzeń to przestrzeń komunikacyjna utworzona przez globalne połączenie sprzętu służącego do automatycznego przetwarzania cyfrowych danych.

3 Matusz Witański | TÜV NORD Polska Sp. z o.o. | Łódź, 2022.06.03



3

Cyberbezpieczeństwo w z informatyzowanym środowisku pracy

Komputer to podstawowe narzędzie pracy, ale także podstawowe narzędzie w nauce i spędzaniu wolnego czasu.

Z komputera obecnie w różnych formach korzystamy praktycznie w każdym miejscu, gdzie przebywamy

Telefon komórkowy i różne urządzenia mobilne (smartfon, smartwatch, tablet itp.) coraz częściej zastępują w życiu codziennym komputery

Ze względu na swój rozmiar urządzenia mobilne często rozszerzają wachlarz funkcjonalności, jakie daje komputer stacjonarny czy przenośny



=



4 Matusz Witański | TÜV NORD Polska Sp. z o.o. | Łódź, 2022.06.03



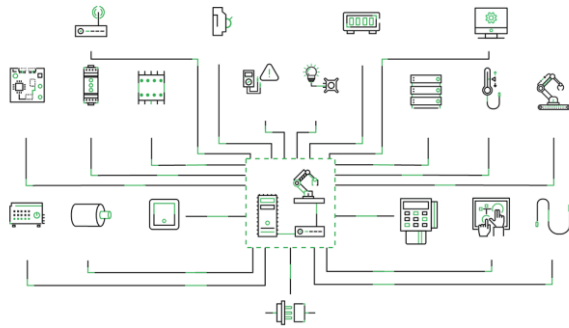
4

Cyberbezpieczeństwo w z informatyzowanym środowisku pracy

Automatyka przemysłowa to, najprościej rzecz ujmując, dziedzina która odpowiada za monitorowanie, sterowanie i nadzorowanie pracy wszelkiego rodzaju maszyn.

Sterowniki PLC w systemach automatyki przemysłowej odgrywają najważniejszą rolę, ponieważ zbierają dane wejściowe i, zgodnie z logiką programu, przetwarzają je na sygnały wyjściowe sterujące urządzeniami wykonawczymi.

Automatyzacja odbywa się niemal we wszystkich sektorach przemysłowych: od urządzeń napędowych, urządzeń do pomiaru i kontroli, poprzez technologię zasilania i połączeń. Rozwój przemysłu będzie powodował coraz większą synergię maszyn i IT.



5 Mateusz Witański | TÜV NORD Polska Sp. z o.o. | Łódź, 2022.06.03



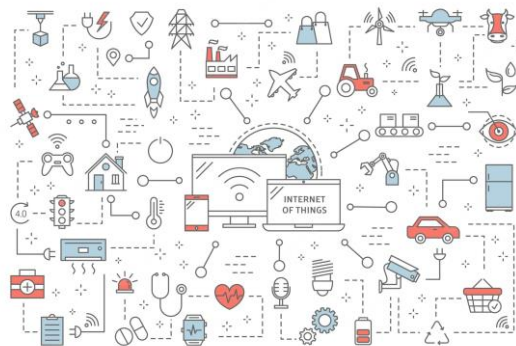
5

Cyberbezpieczeństwo w z informatyzowanym środowisku pracy

Internet Rzeczy to cyfrowa sieć tworzona przez połączone ze sobą przedmioty i zarazem sieć łącząca się ze światem zewnętrznym. O Internecie Rzeczy mówimy nie tylko, gdy my komunikujemy się ze sprzętem, lecz także gdy poszczególne urządzenia komunikują się ze sobą.

Inteligentny dom (smart home) to zbiorcza nazwa dla systemów i urządzeń do automatyki domowej. Innymi słowy, inteligentny dom to taki, z którym użytkownicy są w stanie się porozumieć i któremu mogą wydawać różnego rodzaju polecenia.

Inteligentne miasto (smart city) to miasto, które wykorzystuje technologie informacyjno-komunikacyjne w celu zwiększenia interaktywności i wydajności infrastruktury miejskiej i jej komponentów składowych, a także do podniesienia świadomości mieszkańców.



6 Mateusz Witański | TÜV NORD Polska Sp. z o.o. | Łódź, 2022.06.03



6

Cyberbezpieczeństwo w z informatyzowanym środowisku pracy

Przetwarzanie w chmurze (Cloud Computing) - zasada działania polega na przeniesieniu całego ciężaru świadczenia usług IT na serwer i umożliwienie stałego dostępu poprzez komputery klienckie. Pojęcie chmury nie jest jednoznaczne, w szerokim znaczeniu przetwarzanym w chmurze jest wszystko co jest przetwarzane na zewnątrz zapory sieciowej.

- Infrastruktura jako usługa (Infrastructure as a Service, IaaS)
- Platforma jako usługa (Platform as a Service, PaaS)
- Oprogramowanie jako usługa (Software as a Service, SaaS)
- Komunikacja jako usługa (Communications as a Service, CaaS)



7 Mateusz Witański | TÜV NORD Polska Sp. z o.o. | Łódź, 2022.06.03



7

Cyberbezpieczeństwo w z informatyzowanym środowisku pracy

Człowiek najsłabszym ogniwem w procesie bezpieczeństwa informacji:

- tworzy oprogramowania dla urządzeń i maszyn
- konfiguruje ustawienia maszyn i urządzeń
- korzysta w miarę swoich umiejętności z urządzeń i maszyn
- odpowiada za prawidłowe działanie urządzeń i maszyn



8 Mateusz Witański | TÜV NORD Polska Sp. z o.o. | Łódź, 2022.06.03



8

Cyberbezpieczeństwo w z informatyzowanym środowisku pracy

Bezpieczeństwo pracy

Bezpieczeństwo pracy to zespół warunków, które powinny być zachowane w zakładzie pracy, aby pracownicy mogli wykonywać swoje zadania bezpiecznie i bez szkody dla zdrowia. W znacznej mierze zależy ono od przeszkolenia i postępowania pracowników.

Pracodawca jest obowiązany chronić zdrowie i życie pracowników przez zapewnienie bezpiecznych i higienicznych warunków pracy przy odpowiednim wykorzystaniu osiągnięć nauki i techniki. Natomiast pracownik jest zobowiązany do przestrzegania zasad bezpieczeństwa i higieny pracy.

Zarządzanie ciągłością działania to zbiór działań jakie podejmuje organizacja w celu zapewnienia klientom, dostawcom i pracownikom dostępności jej krytycznych funkcji biznesowych w przypadku wystąpienia zakłócenia. Zarządzanie ciągłością działania odnosi się do czynności wykonywanych codziennie, mających na celu zapobieganie wystąpienia sytuacji awaryjnej oraz utrzymywanie gotowości do natychmiastowej reakcji gdyby takowa zaistniała.

Cyberbezpieczeństwo w z informatyzowanym środowisku pracy

Cyberbezpieczeństwo

Cyberbezpieczeństwo to ogół technik, procesów i praktyk stosowanych w celu ochrony sieci informatycznych, urządzeń, programów i danych przed atakami, uszkodzeniami lub nieautoryzowanym dostępem.

Cyberbezpieczeństwo bywa także określane jako „bezpieczeństwo technologii informatycznych”. Jest to odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy. Stanowi również zespół zagadnień związanych z zapewnianiem ochrony w obszarze cyberprzestrzeni.

Cyberbezpieczeństwo to proces, którego celem jest ochrona danych i systemów wewnętrznych firm przed zagrożeniami, jakie niosą za sobą cyberataki. Wdrożenie odpowiednich procedur w tym zakresie pozwala zapobiec skutkom działań cyberprzestępców, które mogą wyrządzić organizacji wiele szkód.

Cyberbezpieczeństwo w z informatyzowanym środowisku pracy

Co nam zagraża w cyberprzestrzeni?

- SPAM czyli niechciana korespondencja
- Phishing czyli bezpośrednie wyłudzenie poufnych informacji lub za pomocą złośliwego oprogramowania
- Kradzież tożsamości
- Wyciek danych, w tym danych osobowych i danych wrażliwych
- Ataki ransomware w celu wyłudzenia okupu za odszyfrowanie lub nieujawnianie wykradzionych danych
- Ataki DDoS czyli blokowanie dostępu do usług poprzez sztuczne generowanie wzmożonego ruchu

11 Mateusz Witański | TÜV NORD Polska Sp. z o.o. | Łódź, 2022.06.03



11

Cyberbezpieczeństwo w z informatyzowanym środowisku pracy

Co nam zagraża w cyberprzestrzeni?

- Naruszenie autentyczności, integralności lub dostępności danych
- Świadome i nieświadome zagrożenia powodowane przez pracowników
- Fizyczne uszkodzenia i/lub kradzież urządzeń i maszyn
- Przerwanie ciągłości pracy maszyn i urządzeń spowodowane utratą dostępności do sieci energetycznej i/lub teleinformatycznej
- Brak lub utrudniony dostęp do informacji
- Cyberszpiegostwo

12 Mateusz Witański | TÜV NORD Polska Sp. z o.o. | Łódź, 2022.06.03



12

Cyberbezpieczeństwo w z informatyzowanym środowisku pracy

Stosuj zasadę ograniczonego zaufania

W cyberprzestrzeni, tak jak na drodze, nie można ufać bezgranicznie nikomu. Zawsze upewnij się, z kim masz do czynienia i czy osoba jest tą, za którą się podaje. Jeżeli nie jesteś pewien, nie podejmuj interakcji.



13 Mateusz Witański | TÜV NORD Polska Sp. z o.o. | Łódź, 2022.06.03

13

Minimalizuj przekazywanie danych

Nie przekazuj danych wtedy, kiedy nie jesteś przekonany, że jest to niezbędne. W sytuacji, gdy musisz przekazywać dane, przekazuj tylko te, które są niezbędne oraz w taki sposób, żeby mieć pewność, że nie dostaną się w niepowołane ręce.



Cyberbezpieczeństwo w z informatyzowanym środowisku pracy

Stosuj się do przepisów i procedur

Stosowanie się do przyjętych w miejscu pracy przepisów i procedur pozwoli Ci pracować skutecznie i bezpiecznie. Obowiązujące w Twoim miejscu pracy procedury są odzwierciedleniem wiedzy i doświadczenia, jakie mają osoby je tworzące.



14 Mateusz Witański | TÜV NORD Polska Sp. z o.o. | Łódź, 2022.06.03

14

Zabezpiecz swoje urządzenia

Zabezpieczenia wymagają nie tylko komputery. Coraz częściej dostęp do Internetu mają takie urządzenia, jak komórki, zegarki czy urządzenia AGD. Także w przemyśle coraz częściej wykorzystywane jest sterowanie i monitorowanie zdalnie poszczególnych maszyn, jak i całych linii. To także wymaga Twojej uwagi.



Cyberbezpieczeństwo w z informatyzowanym środowisku pracy

Postępuj rozsądnie i ostrożnie

Każde działanie w cyberprzestrzeni wymaga od Ciebie rozsądku. Nie działaj pochopnie, nieostrożnie i lekkomyślnie. Tylko w ten sposób Twoje działania zminimalizują ryzyko wystąpienia niepożądanych konsekwencji poruszania się w cyberprzestrzeni.



Dbaj o swoje urządzenia

Każde urządzenie wymaga uwagi, aby działało poprawnie. Dlatego każde urządzenie należy poddawać okresowym przeglądom, konserwacjom i aktualizacjom oprogramowania. Tylko dobrze utrzymane urządzenia zapewnią prawidłową pracę.



15 Mateusz Witański | TÜV NORD Polska Sp. z o.o. | Łódź, 2022.06.03



15

Cyberbezpieczeństwo w z informatyzowanym środowisku pracy



Certyfikacja systemów ISO 27001, ISO 22301, ISO 20000

Certyfikacja osób: Audytor Wiodący SZBI w Akredytacji PCA

Szkolenia systemowe oraz biznesowe



16 Mateusz Witański | TÜV NORD Polska Sp. z o.o. | Łódź, 2022.06.03



16



Dziękuję za uwagę

