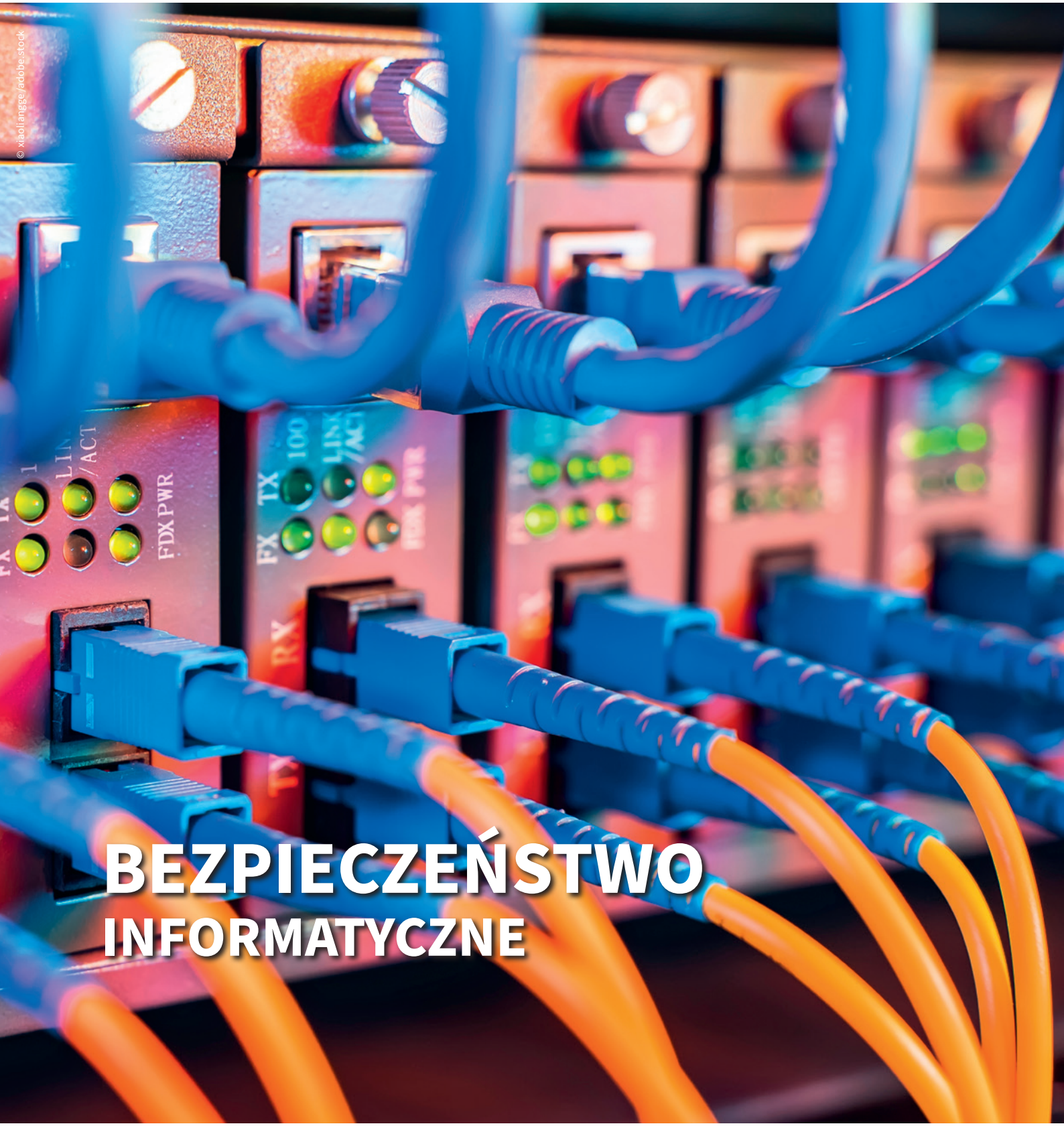
KAN Brief
Kommission Arbeitsschutz und Normung
3/23



BEZPIECZEŃSTWO INFORMATYCZNE

W NUMERZE

© a_korn - stock.adobe.com

Temat tytułowy

Tematy wydania

© GordonGrand - stock.adobe.com

© M.Dörr & M.Frommherz - stock.adobe.com

Bądź na bieżąco:

www_kan_de

Kommission Arbeitsschutz und Normung (KAN)

KAN_Arbeitsschutz_Normung

KAN – Kommission Arbeitsschutz und Normung

Benjamin Pfalz
Przewodniczący KAN
IG Metall

Cyberbezpieczeństwo: wyzwanie regulacyjne i operacyjne

Przedsiębiorstwa muszą chronić się przed cyberatakami bardziej niż kiedykolwiek. Już od dawna to również kwestia bezpieczeństwa pracy. Ze względu na interakcje między człowiekiem a maszyną, z uwagi na stosowanie zdalnie sterowanych środków produkcji, sieciowych systemów produkcyjnych i rosnące wykorzystanie uczenia maszynowego, należy coraz częściej uwzględniać bezpieczeństwo cybernetyczne również w ramach oceny ryzyka operacyjnego. Ogólnie rzecz biorąc, szczególną rolę odgrywają działania na rzecz bezpieczeństwa produktu.

Przepisy w coraz większym stopniu uwzględniają te aspekty. Na przykład w przypadku istotnych dla bezpieczeństwa urządzeń pomiarowych, sterujących i regulacyjnych niemieckie Techniczne zasady bezpieczeństwa w zakładach pracy TRBS 1115 konkretyzują niemieckie Rozporządzenie o bezpieczeństwie w zakładach pracy pod względem określania i zdefiniowania niezbędnych środków bezpieczeństwa cybernetycznego. Jednocześnie tematem zajmują się również nowe unijne rozporządzenie maszynowe i nadchodzące rozporządzenie o sztucznej inteligencji. Tak zwana ustawa o cyberodporności została zainicjowana w celu uregulowania dopuszczenia do obrotu produktów i półproduktów z elementami cyfrowymi.

Teraz standaryzacja musi odpowiednio wspierać poziom rozporządzeń. Mandat normalizacyjny, dotyczący projektu rozporządzenia w sprawie sztucznej inteligencji, wyraźnie porusza temat cyberbezpieczeństwa. Europejskie organizacje normalizacyjne już na to reagują, dokonując przeglądu istniejącego zbioru norm i przydzielając tę sprawę w swoich strukturach.

W żadnym razie nie może tutaj zabraknąć głosu BHP! Dlatego KAN zajmuje się tą kwestią na wszystkich poziomach, przykładowo w prowadzonej jeszcze w tym roku merytorycznej rozmowie na temat istotnej z punktu widzenia BHP normalizacji w kontekście rozporządzenia w sprawie sztucznej inteligencji. «

Rozporządzenie UE: połączony do sieci świat urządzeń i maszyn ma być bardziej bezpieczny

Zgodnie z aktem Komisji Europejskiej dotyczącym cyberodporności producenci produktów „z elementami cyfrowymi" będą musieli zapewnić cyberbezpieczeństwo przez cały cykl życia produktu.

W związku z utrzymującymi się cyberatakami, na przykład za pomocą trojanów szyfrujących, Komisja Europejska nadal nalega na eliminację luk w zabezpieczeniach IT. Po takich ustawach jak uchwalony w 2019 roku akt o cyberbezpieczeństwie, który stanowi podstawę ogólnounijnego programu certyfikacji bezpieczeństwa IT połączonych do sieci urządzeń, systemów i usług, czy najnowsza nowelizacja dyrektywy w sprawie bezpieczeństwa sieci i informacji (NIS2), zainicjowała we wrześniu 2022 r. projekt ustawy o cyberodporności (CRA)[1]. Zgodnie z planowanym rozporządzeniem w sprawie cyberodporności produkty „z elementami cyfrowymi", takie jak sprzęt i oprogramowanie, mają w przyszłości „być wprowadzane do obrotu z mniejszą liczbą podatności".

Zakres obowiązywania projektu jest szeroki. Komisja chce na przykład rejestrować „każde oprogramowanie lub sprzęt komputerowy i związane z nimi zdalne rozwiązania w zakresie przetwarzania danych", w tym powiązane komponenty, nawet jeśli są one wprowadzane do obrotu oddzielnie. Oczekuje się, że do priorytetów należeć będą Internet rzeczy lub prywatne małe routery („routery plastikowe"), które jak dotąd są często podatne na ataki ze względu na wiele wbudowanych luk w zabezpieczeniach. Pominięte mają zostać produkty „opracowane wyłącznie do celów bezpieczeństwa narodowego lub do celów wojskowych" lub przeznaczone specjalnie do przetwarzania informacji niejawnych. Akt nie dotyczy również takich sektorów jak lotnictwo, wyroby medyczne czy pojazdy silnikowe, ponieważ w stosunku do nich istnieją już odrębne specyficzne wymogi.

Zgodnie z projektem objęci nim producenci w przyszłości będą musieli spełniać podstawowe wymogi bezpieczeństwa cybernetycznego w zakresie projektowania, rozwoju i procesu produkcji, zanim wprowadzą urządzenie na rynek. Należy ich zachęcać do monitorowania luk w zabezpieczeniach przez cały cykl życia urządzenia i do eliminowania ich za pomocą automatycznych i bezpłatnych aktualizacji. Ponadto producenci mają obowiązek w ciągu zaledwie 24 godzin zgłosić do Agencji Unii Europejskiej ds. Cyberbezpieczeństwa ENISA każdy incydent mający wpływ na bezpieczeństwo sprzętu i oprogramowania. Zasadniczo będzie wprowadzona skoordynowana linia do ujawniania luk w zabezpieczeniach.

Zgodnie z ustawą o cyberodporności należy ograniczyć możliwości ataku na uwzględnione urządzenia i zminimalizować konsekwencje incydentów. Objęte ustawą produkty mają zapewnić poufność danych, na przykład poprzez szyfrowanie. Obowiązkowa ma być ochrona integralności oraz przetwarzania informacji i wartości pomiarowych, które są absolutnie niezbędne do funkcjonowania artykułu.

Poza tymi podstawowymi wymogami brukselska instytucja rządowa zidentyfikowała szczególnie krytyczne obszary wysokiego ryzyka. Dzieli ona odpowiednie produkty na dwie kategorie, dla których ma zostać wprowadzona różna procedura oceny zgodności. Kategoria I obejmuje systemy zarządzania tożsamością, przeglądarki, menedżery haseł, programy antywirusowe, zapory sieciowe, wirtualne sieci prywatne (VPN), zarządzanie siecią, kompleksowe systemy informatyczne, fizyczne interfejsy sieciowe, routery i chipy. Do tego dochodzą systemy operacyjne np. dla smartfonów czy komputerów stacjonarnych, mikroprocesory i Internet rzeczy (IoT) w przedsiębiorstwach, których nie uważa się za szczególnie wrażliwe.

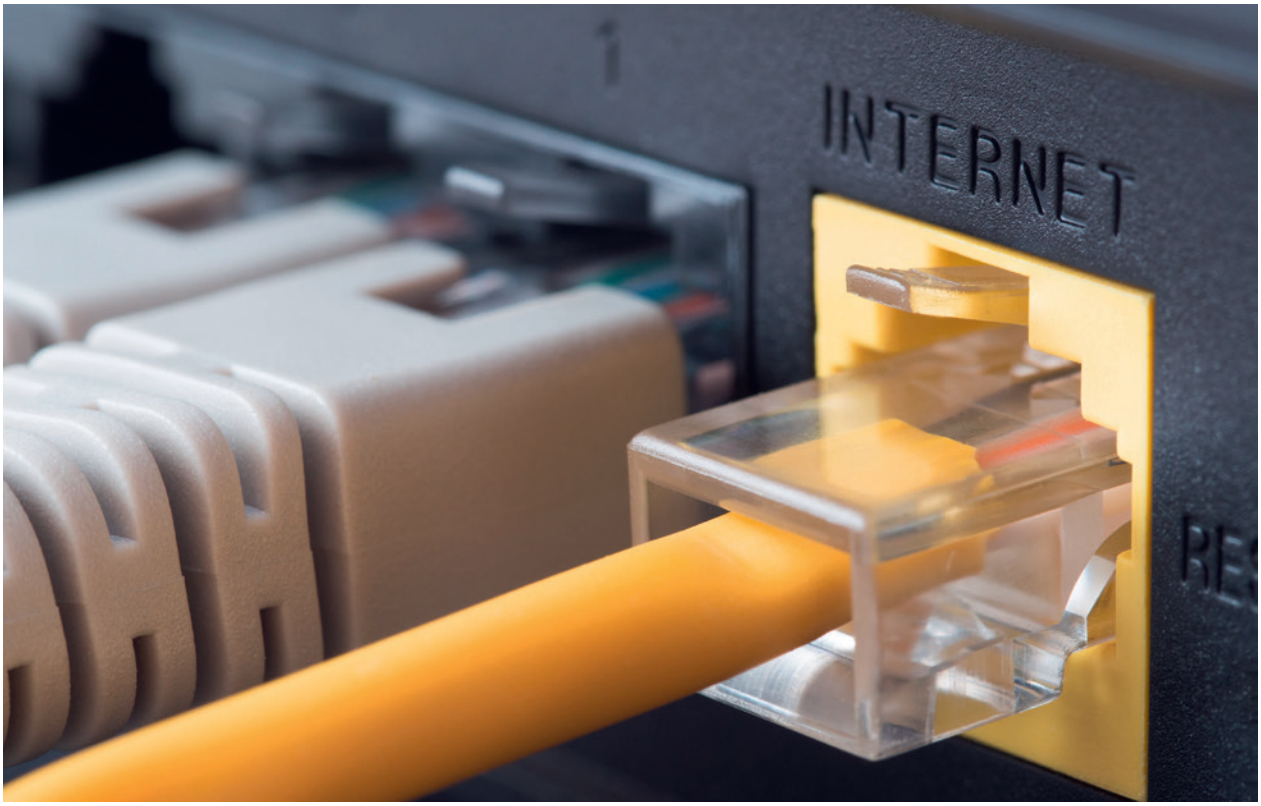
Wyższa kategoria ryzyka II obejmuje urządzenia stacjonarne i mobilne, systemy operacyjne zwirtualizowane i wbudowane np. w maszyny, wystawców certyfikatów cyfrowych, mikroprocesory uniwersalne, czytniki kart, czujniki robotów i inteligentne urządzenia pomiarowe. Ma ponadto obejmować urządzenia IoT, routery i zapory sieciowe do użytku przemysłowego, który zasadniczo jest uważany za „wrażliwe środowisko". Luki w zabezpieczeniach IT mają bowiem już od dawna ogromny wpływ na maszyny i systemy, w coraz większym stopniu podłączone do sieci i dostępne nie tylko na terenie zakładu, wpływając tym samym również na bezpieczeństwo pracy.

Producenci mają przeprowadzać oceny zgodności swoich produktów za pomocą procedury wewnętrznej lub badania przeprowadzonego przez uznane instytucje. Jeśli producent opiera się na normach zharmonizowanych lub otrzymał już certyfikat w ramach europejskiego mechanizmu certyfikacji w zakresie cyberbezpieczeństwa, należy założyć, że odpowiedni sprzęt wzgl. oprogramowanie są zgodne z rozporządzeniem. Importerzy i dystrybutorzy będą mieli obowiązek kontrolować przestrzeganie odpowiednich procedur przez producenta oraz oznakowanie CE urządzenia. W przypadku mniej krytycznych produktów producenci sami będą mogli wystawiać deklarację zgodności. Dla II kategorii ryzyka ma być wymagana opinia strony trzeciej.

Komisja dostrzega potrzebę działania, ponieważ nasilenie cyberprzestępczości już do 2021 r. wygenerowało szacunkowe roczne koszty w wysokości 5,5 bln euro. W powiązanym środowisku incydent cyberbezpieczeństwa dotyczący jednego produktu może mieć szkodliwy wpływ na całe przedsiębiorstwo lub cały łańcuch dostaw i w ciągu kilku minut rozprzestrzenić się poza granice jednolitego rynku, jak miało to miejsce na przykład w przypadku złośliwego oprogramowania komputerowego WannaCry. Mogłoby to zatrzymać działalność gospodarczą i społeczną, a nawet stanowić zagrożenie dla życia.

Krytyka projektu rozporządzenia

Niemiecki Ustawowy Zakład Ubezpieczeń od Następstw Nieszczęśliwych Wypadków (DGUV) w swoim oświadczeniu [2] skrytykował fakt, że już kluczowe pojęcie cyberbezpieczeństwa nie zostało jasno zdefiniowane. W różnych normach i rozporządzeniach jest ono naprzemiennie rozumiane jako stan, czynność lub produkt. Zasadniczo problematyczne są słowa, w których skład wchodzi cząstka „cyber", a które nie zostały precyzyjnie zdefiniowane. Przykładowo ataki przez radio lub interfejsy USB - w zależności od źródła - nie zostały objęte terminem cyberbezpieczeństwa.



© a_korn - stock.adobe.com

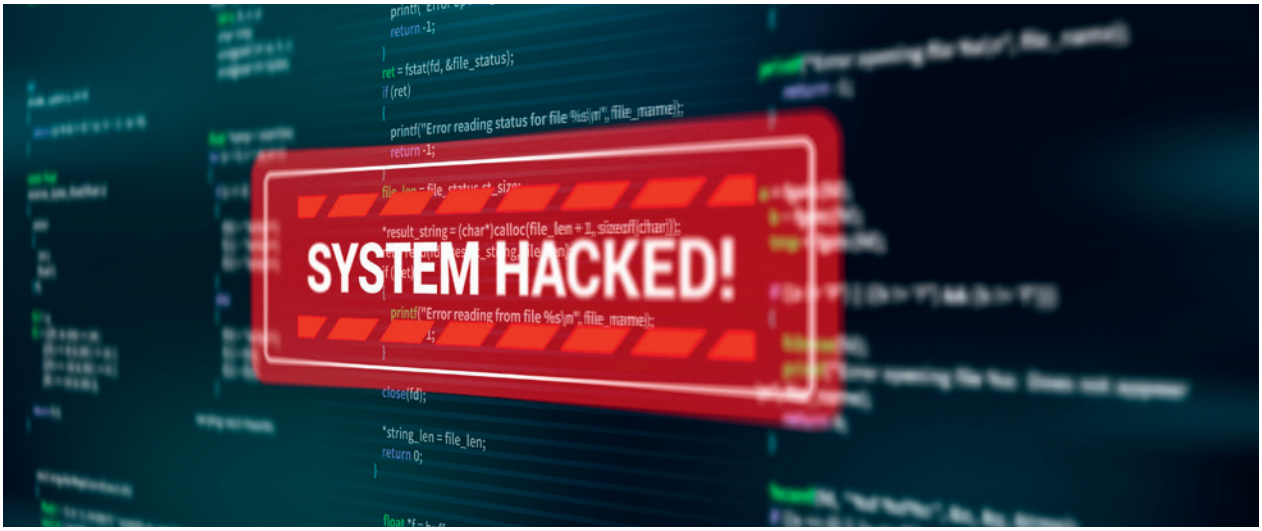
DGUV krytycznie odnosi się również do obowiązku zgłaszania przez producentów w ciągu 24 godzin szczegółowych informacji na temat danej luki w zabezpieczeniach. Przeprowadzenie analizy w tak krótkim czasie jest w wielu przypadkach nierealne. Poza tym przesyłanie szczegółów, które mogą zostać wykorzystane do ataków, nie jest bezwzględnie konieczne. W swoim oświadczeniu DGUV opowiada się za przekazywaniem tylko tych danych, które są naprawdę potrzebne władzom, na przykład w celu ostrzeżenia przed produktem lub oceny skutków luki. Również planowany dwuletni okres na dostosowanie się do nowych wymagań jest w opinii Ustawowego Zakładu Ubezpieczeń od Następstw Nieszczęśliwych Wypadków zbyt krótki dla producentów, którzy są uzależnieni od innych produktów i muszą czekać na przykład na ocenę zgodności.

Ponadto systemów operacyjnych nie można sensownie przetestować, ponieważ nieustannie ewoluują, ostrzega Jonas Stein, kierownik zespołu roboczego ds. bezpieczeństwa w DGUV. Często są przy tym uzależnione od open source, na przykład w Linuksie. W przypadku wolnego oprogramowania nie ma jednak tylko jednego producenta, który odpowiadałby za procedurę zgodności. Sama scena open source obawia się wpadnięcia w pułapkę odpowiedzialności, ponieważ wielu indywidualnych programistów bierze udział we wspólnych pracach i za potencjalne luki musieliby odpowiadać wszyscy. Europejska Fundacja Wolnego Oprogramowania (FSFE) skarży się: „Ze względu na brak funduszy i zasobów, aby poddać się proponowanym procedurom zgodności CE, niektóre z tych projektów mogą zostać całkowicie wstrzymane”.

Rada Ministrów UE i przedmiotowo właściwa Komisja Parlamentu Europejskiego ds. Przemysłu w połowie lipca zajęły stanowisko w sprawie propozycji Komisji, dzięki czemu wkrótce mogą rozpocząć się negocjacje w sprawie ostatecznego kompromisu. Państwa członkowskie apelują o uproszczoną deklarację zgodności, większe wsparcie dla małych przedsiębiorstw i uściślenie spodziewanej żywotności produktów przez producentów. Ponadto wykorzystane luki w zabezpieczeniach oraz incydenty związane z bezpieczeństwem nie mają być zgłaszane do Agencji Unii Europejskiej ds. Cyberbezpieczeństwa ENISA, tylko do właściwych organów krajowych. Posłowie z kolei wzywają żądają bardziej precyzyjnych definicji, realnych harmonogramów i bardziej sprawiedliwego podziału kompetencji. Z drugiej strony apelują o to, aby również urządzenia do inteligentnego domu, smartwatche i prywatne kamery bezpieczeństwa zostały umieszczone w kategorii wysokiego ryzyka.

Dr Stefan Krempl
Niezależny dziennikarz
sk@nexttext.de

[1] https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=celex%3A52022PC0454
[2] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13410-Akt-dotyczacy-cyberodpornosci-nowe-przepisy-dotyczace-cyberbezpieczenstwa-produktow-cyfrowych-i-us%C5%82ug-pomocniczych/F3376532_pl



Ugruntowana wiedza w zakresie nowych specyfikacji bezpieczeństwa przemysłowego

Komponenty bezpieczeństwa funkcjonalnego chronią życie i zdrowie ludzi, na przykład uniemożliwiając im dostęp do niebezpiecznych obszarów maszyn i urządzeń. Ważne jest, aby również ingerencje z zewnątrz nie wpływały negatywnie na bezpieczeństwo. W tym celu należy konsekwentnie wdrażać najnowocześniejsze rozwiązania, a producenci i operatorzy muszą odpowiednio reagować w przypadku luk w zabezpieczeniach.

Aby funkcje bezpieczeństwa sterowników mogły działać niezawodnie, również sam sterownik musi być bezpieczny – czyli zabezpieczony przed awarią i manipulacją. Przeraża wzrost częstotliwości nowych komunikatów o katastrofach w obszarze bezpieczeństwa przemysłowego. Jednak istnieje powód do nadziei, ponieważ przy obecnym stanie techniki właściwie bardzo łatwo można uniknąć praktycznie wszystkich luk w zabezpieczeniach, jak pokazuje poniższy typowy przykład.

Już w 1883 roku Auguste Kerckhoffs opracował sześć podstawowych warunków poufnej komunikacji. Drugi warunek brzmiał: „System nie może wymagać tajności i powinien móc bez szkody wpaść w ręce wroga". Guglielmo Marconi najwyraźniej nie znał tej pracy. Jego telegrafia do poufnej komunikacji wymagała, aby nikt nie wszedł w posiadanie żadnego z urządzeń, nie zrekonstruował żadnego z nich i nie ustawił go na tej samej częstotliwości. W 1903 roku Nevil Maskelyne zwrócił uwagę na ten problem, wtrącając przesłane alfabetem Morse'a wulgarne wiadomości podczas występu Marconiego, przez co został uznany za jednego z pierwszych hakerów. Chociaż bezpieczne szyfrowanie przy użyciu metod kryptograficznych jest znane już od dawna, tę samą wadę projektową można spotkać również dziś w sterownikach radiowych do systemów sygnalizacji świetlnej[1] lub dźwigów przemysłowych[2].

Brak jednolitej definicji pojęć

Wyszukiwarka norm i standardów związanych z bezpieczeństwem Uniwersytetu w Bremie[3] ma obecnie w swojej bazie danych około 800 norm i ponad 2000 wyników wyszukiwania dotyczących przepisów prawnych. Problem w tym, że w dokumentach stosowane są różne pojęcia, których częściowo nie definiuje się jednoznacznie. Podczas gdy niektóre dokumenty obszernie omawiają kwestie bezpieczeństwa wzgl. bezpieczeństwa informacji, inne tworzą neologizmy w formie kontaminacji składającej się z prefiksu „cyber" i innego słowa. Te nowo utworzone słowa należy precyzyjnie zdefiniować w dokumencie, ponieważ same w sobie nie mają unikalnego znaczenia. Czasem „cyberbezpieczeństwo" oznacza działanie, innym razem zabezpieczenie przed atakami z Internetu, jeszcze innym stan, w którym produkt jest chroniony przed atakami drogą radiową.

Lepiej pracować z jednoznacznymi pojęciami „bezpieczeństwo informacji" wzgl. „bezpieczeństwo" niż tworzyć nowe słowa. Jeżeli zakres znaczenia ma zostać zredukowany na przykład do ataków drogą radiową, należy jasno zdefiniować to ograniczenie. Inne, bardzo eleganckie rozwiązanie wybrało rozporządzenie UE w sprawie maszyn, które w załączniku III 1.1.9 wymaga „zabezpieczenia przed uszkodzeniem" i jest w tej kwestii bardziej jednoznaczne niż dotychczasowa dyrektywa maszynowa UE. Rozporządzenie koncentruje się przy tym na celu ochrony, aby na przykład podczas zdalnego dostępu nie dochodziło do sytuacji zagrożenia, i pozostawia otwartą kwestię, co konkretnie było przyczyną uszkodzenia.

Szybka komunikacja jest kluczowa

Szybka i skuteczna komunikacja jest kluczem do odpowiedniej reakcji na luki w zabezpieczeniach. Jednak jak bardzo źle wygląda komunikacja, okazało się w grudniu 2021 r., kiedy to było głośno o luce w zabezpieczeniach biblioteki Log4J. Ta biblioteka języka oprogramowania jest nie tylko częścią wielu usług serwerowych, lecz również licznych komponentów przemysłowych. Choć z jednej strony pojawiały się zarzuty, że biblioteka była wykorzystywana niewłaściwie i że przeczytanie dokumentacji pozwoliłoby zapobiec problemom związanym z bezpieczeństwem, wielu producentów równocześnie zastanawiało się, czy luki w zabezpieczeniach dotyczą również ich. Nierzadko producenci potrzebowali kilku miesięcy, by dowiedzieć się, czy ich produkty też są dotknięte tym problemem.

Jonas Stein

Kierownik laboratorium badawczego ds. bezpieczeństwa przemysłowego i kierownik grupy roboczej ds. bezpieczeństwa niemieckiego ustawowego zakładu ubezpieczeń od następstw nieszczęśliwych wypadków DGUV

Jonas.Stein@dguv.de

Reasumując, zabrakło

- kontaktu alarmowego ds. bezpieczeństwa wewnątrz przedsiębiorstwa,
- jednolitego formatu zaleceń dotyczących postępowania oraz
- standardu umożliwiającego również producentom zgłaszanie, że luka w zabezpieczeniach nie dotyczy określonego produktu.

Problem braku jednolitych informacji i interfejsów został rozwiązany za pomocą zestawu otwartych specyfikacji, opracowanych przez różne grupy przedsiębiorstw, instytucji i organizacji, i możliwych do natychmiastowego wdrożenia przez każde przedsiębiorstwo (zob. tabela). Zgodny ze specyfikacją IETF RFC 9116 kontakt alarmowy jest przechowywany w prostym pliku security.txt na stronie internetowej [4]. Producent może w nim również umieścić odnośnik do swojej listy zaleceń postępowania (CSAF). Każdy sprzęt i każde oprogramowanie otrzymują unikalny globalny identyfikator (CPE), dzięki czemu międzynarodowe alerty (CVE) są automatycznie przypisywane do konkretnych produktów i wersji. Krytyczność luki w zabezpieczeniach zostaje sklasyfikowana tak dobrze, jak to możliwe za pomocą jednolitego na całym świecie wskaźnika (CVSS). Dzięki otwartej specyfikacji SPDX można udokumentować w formie dostosowanej do odczytu maszynowego, które biblioteki zostały użyte w poszczególnych projektach. Oprogramowanie po stronie operatora może następnie regularnie sprawdzać w odniesieniu do wszystkich produktów, czy występują alerty bezpieczeństwa oraz wyświetlać zalecenia dotyczące postępowania.

Kilka dużych przedsiębiorstw już stawia na te specyfikacje. Teraz ważne jest, aby wszystkie inne firmy szybko poszły w ich ślady, żeby informacja o problemach związanych z bezpieczeństwem następowała szybko i w niedrogi sposób.

W pierwszej kolejności przedsiębiorstwa powinny przynajmniej zapewnić swoją dostępność na wypadek incydentów związanych z bezpieczeństwem i opublikować kontakt alarmowy. Dzięki instrukcjom dostępnym na stronie https://cert.dguv.de można to wdrożyć w ciągu kilku minut.

Informacja wejściowa	Aktualizacja	Specyfikacja
Własny kontakt alarmowy	Producent, operator	„security.txt“ RFC 9116
Identyfikator wyrobu / ID (nazwa producenta, nazwa produktu, wersja, wersja językowa, ...)	Producent	CPE
Wykaz komponentów oprogramowania (Software Bill of Materials - SBOM)	Producent	SPDX
Powiadomienie o luce w zabezpieczeniach	Jednostki ds. nadawania numerów CVE	CVE
Security Advisory (zalecenie dotyczące postępowania z CVE)	Producent	CSAF
Cechy służące do oceny krytyczności	Producent	CVSS

Zestaw otwartych specyfikacji, które łącznie w decydujący sposób przyczynią się do bezpieczeństwa przemysłowego. W najbliższych latach nadadzą one komunikacji na temat luk w zabezpieczeniach pilnie potrzebne tempo.

[1] Raport telewizji ARD o hakerach zmieniających sygnalizację świetlną w Hanowerze na zieloną (2021), https://ardmediathek.de Hacker Ampeln
[2] Andersen et al, 2019, A Security Analysis of Radio Remote Controllers for Industrial Applications https://documents.trendmicro.com/assets/white_papers/wp-a-securityanalysis-of-radio-remote-controllers.pdf
[3] https://cybersecurity-navigator.de
[4] Krytyczne luki w zabezpieczeniach maszyn i instalacji oraz plik security.txt: https://cert.dguv.de

Nowe rozporządzenie w sprawie maszyn - konsekwencje dla zharmonizowanej normalizacji

W prawie żadnym innym sektorze przemysłowym normy nie mają tak dużego znaczenia jak w przemyśle maszynowym. Nowe rozporządzenie UE w sprawie maszyn stawia komitety normalizacyjne przed wielkim zadaniem, polegającym na sprawdzeniu zgodności norm z nową podstawą prawną oraz, w razie potrzeby, podejmowaniu działań w celu ich dostosowania.

Wymagany przez użytkowników wysoki poziom bezpieczeństwa podczas obsługi maszyn - w połączeniu z różnorodnością typów maszyn - z biegiem lat doprowadził do zdumiewająco dużej liczby sięgającej ponad ośmiuset zharmonizowanych norm w ramach europejskiej dyrektywy maszynowej. Użytkownicy mogą przyjąć, że zawarte w nich rozwiązania i środki są odpowiednie, aby spełniać ustawowe wymogi rozporządzeń lub dyrektyw, dla których zostały opracowane. Spośród tych ponad ośmiuset norm około sto tak zwanych norm typu B dotyczy określonych aspektów bezpieczeństwa lub urządzeń zabezpieczających, odnoszących się do wielu maszyn. Ponad siedemset norm opisuje wymagania i rozwiązania techniczne dla konkretnych typów maszyn (normy typu C). Dzięki współdziałaniu dyrektywy maszynowej i zharmonizowanych norm na przestrzeni lat ugruntował się sprawdzony system, zapewniający produktom maszynowym uznany na całym świecie wysoki poziom bezpieczeństwa.

Standaryzacja stoi przed gigantycznym zadaniem

Wraz z opublikowanym w Dzienniku Urzędowym UE 29 czerwca 2023 r. nowym rozporządzeniem UE 2023/1230 w sprawie maszyn Komisja Europejska rozpoczęła nowy rozdział w dziedzinie przepisów prawnych. 20 stycznia 2027 r. rozporządzenie maszynowe zastąpi dotychczas obowiązującą dyrektywę maszynową 2006/42/WE w trybie terminu ostatecznego – czyli bez okresu przejściowego. Oprócz licznych formalnych i koncepcyjnych korekt tekstu prawnego istotnych zmian dokonano także w załączniku I do dyrektywy maszynowej, opisującym zasadnicze wymagania w zakresie ochrony zdrowia i bezpieczeństwa (EHSR – Essential Health and Safety Requirements). W rozporządzeniu maszynowym EHSR można znaleźć w nowym załączniku III. Spełnienie tych wymogów bezpieczeństwa jest głównym zadaniem zharmonizowanych norm. Zmiany nieuchronnie rodzą następujące pytania:

Jaki bezpośredni wpływ mają nowe i zmienione EHSR na treść dzisiejszych zharmonizowanych norm? Czy normy zharmonizowane z dyrektywą maszynową nadal mogą być stosowane w ramach rozporządzenia maszynowego i czy zachowują domniemanie zgodności?

Niełatwo odpowiedzieć na pierwsze pytanie, ponieważ szczegóły praktycznego wzgl. normatywnego wdrażania nowych EHSR „Zabezpieczenie przed uszkodzeniem", „Funkcja nadzoru autonomicznych maszyn mobilnych" czy „Zapobieganie ryzyku związanemu z zetknięciem się z napowietrznymi liniami elektroenergetycznymi pod napięciem" nadal są przedmiotem intensywnych dyskusji.

Jednak ogólny zarys zakresu obowiązywania norm pokazuje, że nowe lub mocno zmodyfikowane EHSR nie pominą praktycznie żadnej kategorii maszyn. Należałoby zatem sprawdzić wszystkie zharmonizowane normy pod kątem adekwatności nowych EHSR i, w razie zasadności, dostosować je zgodnie z przepisami proceduralnymi Komisji UE (tabelaryczny załącznik ZA, datowane odnośniki) zarówno pod względem treści, jak i formy. Teoretycznie wymagałoby to rewizji prawie wszystkich z około 800 zharmonizowanych norm – każdorazowo wraz z kompleksową oceną przeprowadzoną przez konsultantów HAS. Wykonanie tego w trzy i pół roku, jakie pozostały do dnia, z którym zacznie obowiązywać rozporządzenie maszynowe, jest zupełnie nierealne.

Ograniczony wykaz możliwym rozwiązaniem tymczasowym

Dlatego Komisja Europejska planuje – stan na sierpień 2023 r. – w nadzwyczajnym trybie zbiorczo przenieść wszystkie normy europejskie (zarówno EN, jak i EN ISO), które w terminie jeszcze nieustalonym w pierwszej połowie 2026 r. będą zharmonizowane z dyrektywą maszynową, pod nowe rozporządzenie maszynowe jako normy zharmonizowane z tym rozporządzeniem. Jedyne ograniczenie: normy te mogą

oczywiście zapewnić harmonizację tylko dla tych EHSR, które odnoszą się do nich już w ramach dyrektywy maszynowej. Aby wyraźnie zaznaczyć to użytkownikom norm w wykazie w Dzienniku Urzędowym, odpowiedzialne komitety techniczne (TC) będą musiały poddać przeglądowi (NIEKONIECZNIE rewizji) całe swoje portfolio norm w celu zidentyfikowania poszczególnych luk w stosunku do nowego rozporządzenia maszynowego. Jednocześnie w CEN i CENELEC rozpoczną się prace nad stworzeniem normatywnych rozwiązań dla nowych wzgl. istotnie zmodyfikowanych EHSR, tak aby można było normatywnie zlikwidować zidentyfikowane luki.

Obecnie za pomocą koordynującego forum branżowego CEN/CENELEC „Maszyny" opracowywane są wytyczne, mające pomóc TC w tym bardzo ambitnym zadaniu. Wytyczne powinny być dostępne najpóźniej z końcem 2023 roku.

Oczywiście już dziś możliwe i wskazane jest dążenie do zgodności przyszłych rewizji norm lub nowych projektów z nowym rozporządzeniem maszynowym. Należy zatem mieć nadzieję, że do początku 2027 r. rzeczywiście pewna część norm zostanie dostosowana do nowego rozporządzenia maszynowego. Dla większości zharmonizowanych norm będzie to jednak możliwe dopiero, gdy rozporządzenie maszynowe będzie musiało być już stosowane.

Wraz z nowym mandatem normalizacyjnym Komisji Europejskiej dla rozporządzenia maszynowego należy się spodziewać bardziej precyzyjnych ram czasowych dla przyszłych rewizji norm, które mają być dostępne w nadchodzącym roku. W przeciwieństwie do poprzednich mandatów ten mandat normalizacyjny jest ograniczony czasowo (prawdopodobnie na 5 do 10 lat). Stanowi on fundament prawny, na którym można tworzyć zharmonizowane normy do nowego rozporządzenia maszynowego. Z końcem czerwca opublikowany został pierwszy projekt mandatu normalizacyjnego. Przewiduje się, że komentarze zainteresowanych stron będą jesienią przedmiotem dyskusji odpowiednich gremiów komisyjnych.

Kolejnym środkiem ma być ponadto ułatwienie użytkownikom norm przejścia zharmonizowanych norm spod dyrektywy maszynowej pod rozporządzenie maszynowe. Normy opublikowane między 2024 r. a pierwszą połową 2026 r., mają zawierać dwa załączniki ZA – po jednym dla dyrektywy maszynowej i jednym dla rozporządzenia maszynowego – z których będzie wynikać, do jakich przepisów prawnych odnoszą się poszczególne sekcje normy. Również w tym zakresie zainteresowane normalizacyjne TC zostaną niebawem poinformowane.

Wszystkie opisane środki przyczyniają się do jak najbardziej płynnego przeniesienia zharmonizowanych norm ze starej dyrektywy maszynowej do nowego rozporządzenia maszynowego.

Dr Frank Wohnsland

VDMA

Prezes forum branżowego CEN/CENELEC „Maszyny"

frank.wohnsland@vdma.org

© Arto - stock.adobe.com

Ergonomia cyfrowa: Projekt KAN podsumowuje stan badań

Na zlecenie KAN spółka BioMath GmbH zbadała aktualny stan badań nad interfejsami i formatami danych do cyfrowych modeli człowieka i systemów wykrywania ruchu.

W dziedzinie bezpieczeństwa pracy do planowania i oceny produktów i procesów wykorzystuje się modele i metody cyfrowe. Cyfrowe modele człowieka symulują fizyczne aspekty pracy. Ponadto istnieją systemy, które na podstawie współrzędnych ludzkich stawów rejestrują ruchy w przestrzeni trójwymiarowej. Dane te można następnie wprowadzić do cyfrowego modelu człowieka. Na jego podstawie eksperci opracowują środki służące tworzeniu bezpiecznych i zdrowych stanowisk pracy.

Zarówno instytuty badawcze, jak i przedsiębiorstwa dysponują metodami i narzędziami do analizy, oceny i prezentacji danych z cyfrowych modeli człowieka i systemów wykrywania ruchu. Często jednak są to rozwiązania jednostkowe, niekompatybilne ze sobą nawzajem ze względu na różne formaty danych. Od lat sześćdziesiątych dwudziestego wieku w rozmaitych celach opracowano około 150 różnych cyfrowych modeli człowieka (jednak nie wszystkie z nich są jeszcze w użyciu).

Standaryzacja interfejsów
- między cyfrowymi modelami człowieka nawzajem,
- między systemami wykrywania ruchu wzajemnie i
- między cyfrowymi modelami człowieka a systemami wykrywania ruchu

byłaby użyteczna z punktu widzenia BHP, ponieważ można by stworzyć solidniejszą bazę danych, służącą do opracowania środków umożliwiających projektowanie przyjaznych człowiekowi miejsc pracy. Za pomocą jednolitych interfejsów i formatów danych można łączyć dane ruchowe z różnych źródeł i wykorzystywać je do kompleksowych analiz.

Projekt KAN pokazuje różnorodność modeli

W ramach projektu KAN firma BioMath GmbH gromadziła i analizowała publikacje naukowe na temat ergonomii cyfrowej. Chodziło również o wykazanie, które ustalenia dotyczące ergonomii należy uznać za wiarygodne w odniesieniu do cyfrowych modeli człowieka oraz cyfrowego zapisu, oceny i prezentacji danych ruchowych.

Raport[1] zawiera przegląd cyfrowych modeli człowieka oraz ich właściwości i możliwości. Badanie pokazuje, że cyfrowe modele człowieka opierają się na wskaźnikach antropometrycznych z różnych baz danych, odzwierciedlających różne społeczności. Ponadto dane zostały częściowo pogrupowane i/lub podzielone w bardzo różny sposób. Jakość danych determinuje również jakość cyfrowych modeli człowieka.

Ponadto przeanalizowano, które systemy wykrywania ruchu były już przedmiotem badań. Przede wszystkim chodziło przy tym o możliwości wymiany danych. Tutaj badania wykazały, że nie ma do tej pory jednolitej procedury.

W przyszłych projektach badawczych należy zatem bardziej naświetlić bliżej między innymi następujące kwestie:

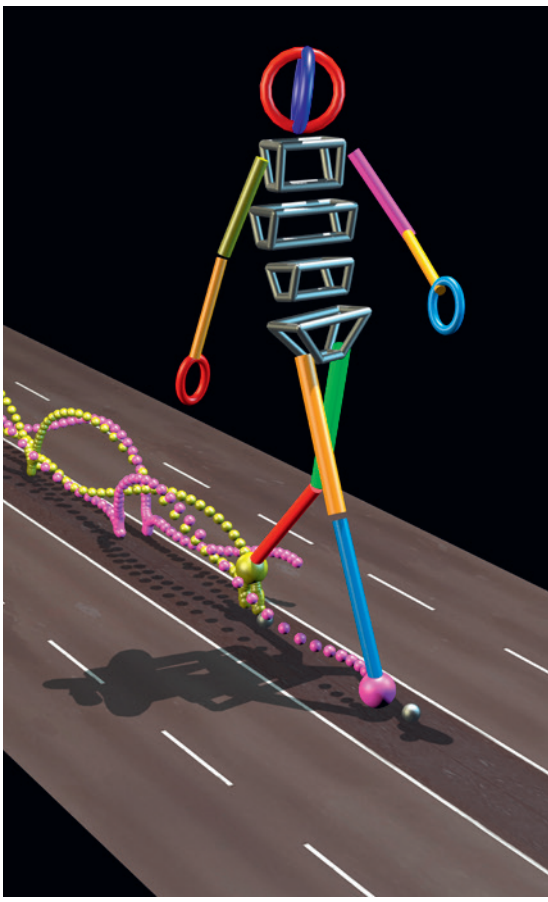
- W odniesieniu do wymiany danych między cyfrowymi modelami człowieka wskazany byłby neutralny dla producenta, dobrze udokumentowany, znormalizowany format.
- Należy zdefiniować pojęcia i możliwe stopnie szczegółowości, np. dla niektórych części cyfrowego modelu człowieka.
- Ponieważ istnieją różne podejścia do właściwości i konfiguracji modeli człowieka, ważne byłyby ustalenia dotyczące struktury modeli, zwiększające ich porównywalność.

Co dalej?

Odbiorca projektu podsumował wyniki badań w raporcie, zawierającym obecny punkt wyjścia i sposoby harmonizacji jednolitych interfejsów i formatów danych. Treść tego raportu ma zostać udostępniona w formie raportu technicznego (DIN/TR). W tym celu KAN przygotuje tekst i złoży wniosek do DIN. Długoterminowym celem jest stworzenie podstawowych norm dla cyfrowych modeli człowieka, interfejsów i formatów danych. Jednak z punktu widzenia KAN pełna harmonizacja wymogów nie jest jeszcze obecnie możliwa.

Katharina von Rymon Lipinski
vonrymonlipinski@kan.de

[1] www.kan.de/fileadmin/Redaktion/Dokumente/KAN-Studie/de/2023_KAN-Projekt_Digitale_Ergonomie_bf_final.pdf



© vrx123 - stock.adobe.com

ASGA – nowa komisja zajmująca się przekrojowymi zagadnieniami z dziedziny BHP

Do istniejących już komisji ds. bezpieczeństwa i higieny pracy w Federalnym Ministerstwie Pracy i Spraw Socjalnych (BMAS) w 2021 r. doszła państwowa Komisja Bezpieczeństwa i Zdrowia w Pracy (ASGA). Jakie są jej zadania i jaki był powód jej powstania?

Państwowe komisje [1] są odpowiedzialne w Niemczech za opracowywanie przepisów (technicznych), konkretyzujących ogólne cele ochrony zawarte w poszczególnych rozporządzeniach do ustawy o bezpieczeństwie i higienie pracy. Komisje, koordynowane przez Federalny Instytut Bezpieczeństwa i Higieny Pracy (BAuA), zajmują się potencjalnymi czynnikami ryzyka w systemie pracy, takimi jak substancje niebezpieczne, substancje biologiczne, miejsca pracy i środki produkcji. Przepisy dostarczają pracodawcom wymogów procesowych i projektowych, których spełnienie jest tożsame z realizacją treści poszczególnych rozporządzeń do ustawy o bezpieczeństwie i higienie pracy (domniemanie zgodności).

Ze względu na dywersyfikację form pracy, cyfryzację i wpływ klimatu na środowisko pracy, dotychczas konsekwentnie wertykalne podejście do regulacji nie wystarcza już do kompleksowej oceny obecnego i przyszłego wpływu na pracowników oraz opracowania właściwych działań. Również w przypadku klasycznych tematów, takich jak ocena ryzyka i szkolenia, wymagania są niezależne od poszczególnych czynników ryzyka i dlatego należy je rozpatrywać (horyzontalnie) z kilku perspektyw.

Potrzeba ta stała się szczególnie widoczna podczas kryzysu wywołanego koronawirusem i związanych z nim nowych wyzwań dla bezpieczeństwa i higieny pracy. Zasada SARS-CoV była pierwszą regułą, która specjalnie została tak opracowana, aby obejmowała wszystkie czynniki. Pomyślne zastosowanie tej zasady w zakładach wyraźnie pokazało, że warto sprawdzać, w jakich innych dziedzinach celowe jest opracowanie horyzontalnych zasad bezpieczeństwa i higieny pracy.

Z tego powodu opublikowane w grudniu 2020 r. uzupełnienie paragrafu 24a zakotwiczyło komisję ASGA[2] bezpośrednio w ustawie o bezpieczeństwie i higienie pracy. Do zadań nowej komisji należy między innymi – o ile nie wchodzi to w zakres odpowiedzialności żadnej innej państwowej komisji – opracowanie zasad i informacji dotyczących sposobu spełnienia wymagań określonych w ustawie o bezpieczeństwie i higienie pracy.

© GordonGrand - stock.adobe.com

Drugim powodem powołania nowej komisji jest brak spójności w dotychczasowych przepisach, wiążący się ze ściśle wertykalnym ukierunkowaniem istniejących komisji. Już w 2011 roku w „Wytycznych w sprawie reorganizacji przepisów i regulacji dotyczących bezpieczeństwa pracy" sformułowano troskę o lepsze skoordynowanie treści autonomicznego prawa statutowego zakładów ubezpieczeń wypadkowych z przepisami państwowymi – zarówno pomiędzy sobą nawzajem, jak i w obrębie obu tych obszarów regulacyjnych. W tym kierunku, w centralnych obszarach działania, jak np. ocenie ryzyka, wciąż jeszcze niewiele się wydarzyło. Wewnątrz ASGA panuje zgoda co do tego, że na tę kwestię należy konsekwentnie zwracać uwagę.

Skład i sposób działania

Skład ASGA nie różni się od składu innych komisji BHP. W komisji reprezentowani są powołani przez BMAS specjaliści publicznych i prywatnych pracodawców, związków zawodowych, organów krajów związkowych, Ustawowego Zakładu Ubezpieczeń od Następstw Nieszczęśliwych Wypadków oraz ze świata nauki. Komisja składa się z 15 członków i 15 zastępców.

Oprócz kierowania komisją przewodniczący ASGA koordynuje współpracę wszystkich komisji BHP w grupie kierowniczej. To gremium odgrywa centralną rolę w opracowywaniu międzysektorowych, horyzontalnych zasad. Komisje -poprzez upoważnione osoby - wnoszą swoją specjalistyczną wiedzę bezpośrednio do danych grup projektowych. W ten sposób są wprost zaangażowane w cały proces, od opracowania zarysu projektu aż po wydanie nowej zasady. To nowość.

ASGA obraduje dwa razy w roku. Grupa kierownicza formułuje swoje argumenty i wyniki głosowań w odpowiednich zaleceniach i przedstawia je grupie koordynacyjnej ASGA. Grupa koordynacyjna analizuje bieżące tematy i zadania i przygotowuje projekty uchwał na posiedzenia ASGA.

Projekty i priorytety

Podobnie jak wszystkie inne komisje, ASGA wyznaczyła sobie program prac na bieżący okres powołania. Główne tematy to ocena ryzyka, stres psychiczny, wydajne i nowoczesne szkolenia, elastyczna pod względem lokalizacji praca przy monitorze poza zakładami pracy oraz wpływ zmian klimatu na bezpieczeństwo i ochronę zdrowia w pracy. Celem jest opracowanie przepisów państwowych, które spójnie wpasowują się w istniejący zbiór przepisów.

Obecnie istnieje wiele wyzwań, ponieważ procesy zmian nigdy nie przebiegają całkowicie płynnie. Celem jest znalezienie właściwej drogi do dobrej, docenianej kultury pracy komitetów, pozwalającej na realizację ambitnego programu prac w drodze konsensusu. Kierownictwo ASGA musi ponadto promować rozwój odpowiednich i przejrzystych procesów i wytycznych, wspierających ten rozwój kultury.

Grupa projektowa „Ocena ryzyka" już pracuje nad koncepcją i treścią zasady ASGA. Grupa projektowa „Stres psychologiczny" planuje rozpocząć prace jeszcze w tym roku.

Prof. dr Anke Kahl

Katedra Bezpieczeństwa Pracy na Uniwersytecie w Wuppertalu

Przewodnicząca ASGA

[1] www.bmas.de/DE/Arbeit/Arbeitsschutz/Arbeitsschutzausschuesse/arbeitsschutzausschuesse.html
[2] www.baua.de/DE/Die-BAuA/Aufgaben/Geschaeftsfuehrung-von-Ausschuessen/ASGA/ASGA_node.html

Reforma unijnego prawa dotyczącego odpowiedzialności za produkt

Jesienią 2022 r. Komisja Europejska zainicjowała modernizację przepisów dotyczących odpowiedzialności za produkt. Po opublikowaniu przez nią projektów nowelizacji dyrektywy w sprawie odpowiedzialności za produkt i nowej dyrektywy w sprawie odpowiedzialności za sztuczną inteligencję Rada Ministrów UE i Parlament Europejski intensywniej zajmują się tym tematem.

Przejście do ery cyfrowej wymaga dostosowania nie tylko ustawodawstwa w sprawie wprowadzania do obrotu, ale także prawa dotyczącego odpowiedzialności. Stara, bo wszak z 1985 r., dyrektywa dotycząca odpowiedzialności za produkt, wdrożona w Niemczech wraz z uchwaleniem ustawy o odpowiedzialności za produkt w 1989 r., nie jest już w stanie pokryć wszystkich szkód wyrządzonych przez produkty. Wynikiem tego jest niepewność prawna przedsiębiorstw i coraz większa liczba produktów, w przypadku których konsument nie ma prawa do odszkodowania za szkodę wyrządzoną przez produkt.[1] Prócz tego dyrektywa ma zostać dostosowana do niedawno zaktualizowanego rozporządzenia w sprawie bezpieczeństwa produktów oraz rozporządzenia w sprawie nadzoru rynku.

Więcej produktów i roszczeń w centrum uwagi

Zakłada się, że nowa dyrektywa w sprawie odpowiedzialności za produkt dotyczyć będzie wszystkich rodzajów produktów – także tych, które wcześniej nie były uwzględnione. Chodzi tu np. również o inteligentne produkty, aktualizacje oprogramowania, systemy sztucznej inteligencji i usługi cyfrowe, ale także o produkty regenerowane i te, które zostały istotnie zmodyfikowane. Producenci gospodarki o obiegu zamkniętym nie będą jednak ponosić odpowiedzialności za szkody spowodowane przez niezmodyfikowane części produktu.

W przypadku produktów z krajów trzecich, np. importowanych do UE bezpośrednio przez konsumentów w drodze handlu elektronicznego, roszczenia z tytułu odpowiedzialności cywilnej ulegają rozszerzeniu. Oprócz obecnie odpowiedzialnych importerów w przyszłości odpowiedzialność cywilna będzie dotyczyła również przedstawicieli producentów i innych podmiotów, takich jak platformy internetowe z siedzibą w UE. Ponadto planowane są zmiany proceduralne: Aby zmniejszyć asymetrię informacji między producentami a konsumentami, podmioty gospodarcze mogą zostać zobowiązane do ujawnienia dowodów. Zasadniczo nastąpi znaczne ułatwienie dowodowe na korzyść poszkodowanych, ale bez odwrócenia ciężaru dowodu. Przewidziane do tej pory górne granice odszkodowań i udziału własnego zostały pominięte.

Dostosowane przepisy o odpowiedzialności

Na podstawie projektu dyrektywy w sprawie odpowiedzialności za produkt roszczenia odszkodowawcze powstają wyłącznie w przypadku obrażeń ciała (w tym uszczerbku na zdrowiu psychicznym), uszkodzenia mienia i utraty danych. Chodzi o rygorystyczną odpowiedzialność za produkt, dotyczącą producenta i innych podmiotów gospodarczych niezależnie od winy. Tylko osoby fizyczne mogą dochodzić roszczeń i tylko wtedy, gdy produkt nie jest wykorzystywany wyłącznie do celów zawodowych.

Nowa dyrektywa w sprawie odpowiedzialności za sztuczną inteligencję uzupełnia ramy prawne

Nowej dyrektywie w sprawie odpowiedzialności za produkt ma towarzyszyć dyrektywa w sprawie odpowiedzialności za sztuczną inteligencję. W przypadku szkód wyrządzonych przez systemy sztucznej inteligencji dyrektywa ma znacznie ułatwić poszkodowanym dochodzenie swoich roszczeń na innej podstawie prawnej niż prawo dotyczące odpowiedzialności za produkt, np. w przypadku naruszeń praw podstawowych lub przepisów o odpowiedzialności cywilnej.

Aby zapobiec powstaniu różnic w przepisach prawnych poszczególnych państw członkowskich UE, należy zapewnić zharmonizowane ramy prawne dotyczące odpowiedzialności producentów, operatorów i użytkowników sztucznej inteligencji. Przewiduje się, że w przypadku szkód za przyczynę będzie się uznawać sztuczną inteligencję. Poszkodowany musi wtedy jedynie wykazać, że dostawca, operator lub użytkownik sztucznej inteligencji nie dopełnił istotnego obowiązku w sposób zawiniony i uprawdopodobnić związek przyczynowy. Ponadto w przypadku procesu producenci wzgl. dostawcy sztucznej inteligencji wysokiego ryzyka będą zobowiązani do dostarczania wszystkich istotnych informacji o produkcie.

Sama dyrektywa w sprawie odpowiedzialności za sztuczną inteligencję nie daje jeszcze prawa do odszkodowania, a raczej uzupełnia istniejące, oparte na winie, krajowe przepisy dotyczące odpowiedzialności w przypadku naruszenia prawa przez sztuczną inteligencję. Nowe przepisy o odpowiedzialności na zasadzie winy pozwalają na uproszczone dochodzenie roszczeń odszkodowawczych.

Negocjacje w instytucjach UE

Rada Ministrów UE zajmowała się już projektem Komisji dotyczącym dyrektywy w sprawie odpowiedzialności za produkt i w dużym stopniu zgadza się z nim. Dyskusja w Parlamencie Europejskim również się rozpoczęła, jednak będzie trwać jeszcze przez kilka miesięcy. Dyrektywa w sprawie odpowiedzialności za sztuczną inteligencję ma być przedmiotem negocjacji dopiero na drugim etapie.

Freeric Meier
meier@kan.de

[1] Badanie ewaluacyjne i propozycje dyrektyw: https://ec.europa.eu/commission/presscorner/detail/pl/ip_22_5807

Wielka Brytania przedłuża ważność oznakowania CE

Brytyjskie Ministerstwo Biznesu i Handlu zapowiedziało przedłużenie okresu uznawania oznakowania CE dla produktów wprowadzanych na rynek w Wielkiej Brytanii (Anglii, Szkocji, Walii) na czas nieokreślony po grudniu 2024 r. Dla Irlandii Północnej okres ten został już przedłużony. Regulacja dotyczy 18 rozporządzeń leżących w gestii ministerstwa, m.in. w sprawie maszyn, środków ochrony indywidualnej, urządzeń ciśnieniowych, urządzeń niskonapięciowych, ATEX i urządzeń gazowych.

Pierwotnie uznanie oznakowania CE w Wielkiej Brytanii miało wygasnąć z końcem 2024 roku i zostać zastąpione obowiązkowym znakiem UKCA (UK Conformity Assessed). Dzięki nowej regulacji przedsiębiorstwa w przyszłości będą mogły wybierać pomiędzy obydwoma oznakowaniami. Jest to korzystne zarówno dla przedsiębiorstw z UE, jak i z Wielkiej Brytanii, ponieważ nie będą musiały certyfikować swoich produktów podwójnie, by móc eksportować je do drugiego obszaru gospodarczego.

Więcej informacji (w języku angielskim): www.gov.uk/government/news/uk-government-announces-extension-of-ce-mark-recognition-for-businesses

Nowa kampania EU-OSHA

W październiku 2023 r. Europejska Agencja Bezpieczeństwa i Zdrowia w Pracy (EU-OSHA) rozpocznie swoją dwuletnią kampanię „Bezpieczeństwo pracy w świecie cyfrowym". EU-OSHA i jej krajowe punkty centralne organizują liczne wydarzenia europejskie i krajowe w celu podnoszenia świadomości w zakresie bezpieczeństwa i higieny pracy wśród pracowników, przedsiębiorstw i decydentów politycznych.

Treść kampanii stanowią: praca na platformach cyfrowych, automatyzacja zadań, praca mobilna i hybrydowa, zarządzanie zasobami ludzkimi z pomocą sztucznej inteligencji i inteligentnych systemów cyfrowych. Celem jest udostępnianie danych i faktów w tym zakresie, mogących ułatwić opracowanie odpowiednich przepisów prawnych, wytycznych, działań informacyjnych i pomocowych oraz nowych usług i produktów.

Informacje na temat kampanii:
https://healthy-workplaces.osha.europa.eu/pl

A+A 2023: KAN też tam będzie!

W dniach 24-27 października 2023 r. w Düsseldorfie odbędą się targi A+A. Firmę KAN będzie można znaleźć na wspólnym stoisku DGUV, w tym roku po raz pierwszy zaprezentowanym publicznościw hali nr 5, stoisko 5C06. Będziemy informować o naszych aktualnych obszarach pracy, takich jak: samojezdne maszyny bezzałogowe, maski chroniące przed infekcjami czy grille gazowe, przedstawimy nasze publikacje i chętnie odpowiemy na pytania dotyczące bezpieczeństwa pracy i standaryzacji.

„Człowiek znormalizowany – zmieniające się wymiary ciała" to temat KAN w „Godzinie rozmów o bezpieczeństwie i zdrowiu" w czwartek 26 października o godzinie 10:00 na scenie wspólnego stoiska DGUV.

Na odbywającym się w tym samym czasie Kongresie A+A KAN zaprezentuje następujące wykłady:

- 25.10.2023: WIZJA ZERO a standaryzacja: deklaracja stanowiska
- 26.10.2023: Istotne dla bezpieczeństwa pracy normy zarządzania poza ISO 45001

Szczegóły programu można znaleźć na stronie www.aplusa-online.com.

Serdecznie zapraszamy!

Prace normalizacyjne w bezpieczeństwie pracy - seminarium podstawowe i specjalistyczne

KAN, we współpracy z Instytutem Pracy i Zdrowia DGUV (IAG), oferuje dwa seminaria na temat normalizacji w obszarze bezpieczeństwa i higieny pracy.

Seminarium podstawowe skierowane jest do aktywnych członków organów normalizacyjnych oraz do wszystkich, którzy chcieliby zajmować się normalizacją dla dobra bezpieczeństwa i zdrowia. Seminarium informuje o procesach związanych z opracowywaniem standardów oraz o możliwościach oddziaływania na nie na poszczególnych etapach. Porady, wskazówki i wzajemna wymiana doświadczeń są filarem udanej współpracy w zakresie normalizacji. Seminarium podstawowe odbędzie się w dniach 25-27 października 2023 r. w Dreźnie.

Znasz podstawy normalizacji i chcesz poszerzyć swoje kwalifikacje? Na seminarium specjalistycznym poznasz innych doświadczonych ekspertów w dziedzinie normalizacji i wspólnie zastanowicie się, za pomocą jakich strategii możecie jeszcze lepiej zoptymalizować swoją (współ-)pracę. Uczestnicy podzielą się swoimi doświadczeniami w zakresie procesu normalizacji i możliwości wywierania wpływu oraz otrzymają aktualne informacje dotyczące normalizacji.

Część stacjonarna seminarium specjalistycznego odbędzie się 5 i 6 grudnia 2023 r. w Dreźnie. Pozostałe części seminarium zostały zaplanowane w formie zdalnej (online) lub w formie pracy autodydaktycznej.

Informacje i zgłoszenia:
https://asp.veda.net/webgate_dguv_prod, numer wydarzenia 570044 (seminarium podstawowe) i 570139 (seminarium specjalistyczne)

Unijne zmiany w normach IEC

Zgodnie z porozumieniem frankfurckim w idealnym przypadku Międzynarodowa Komisja Elektrotechniczna IEC powinna opracowywać normy elektrotechniczne na poziomie międzynarodowym, a Europejski Komitet Normalizacyjny Elektrotechniki CENELEC powinien je równolegle przyjąć jako identyczne normy europejskie (EN IEC). Jednak w niektórych przypadkach przejęcie norm IEC wymaga zmian unijnych, aby możliwe było spełnienie wymogów dyrektyw lub rozporządzeń dotyczących rynku wewnętrznego.

O istnieniu takiej rozbieżności świadczy fakt, że CENELEC nie wydaje tych norm z oznaczeniem EN IEC 6xxxx, lecz jedynie EN 6xxxx – ale z tym samym numerem co IEC.

Wydarzenia

18.-20.10.23 » Dresden

Seminar
Manipulation an Maschinen und Anlagen: Risiken erkennen, Maßnahmen ergreifen
IAG
https://asp.veda.net/webgate_dguv_prod
🔎 570089

19.10.23 » Bern

Tagung
Schweizerische Tagung für Arbeitssicherheit
SUVA
www.suva.ch 🔎 Tagung

24.-27.10.23 » Düsseldorf

Messe und Kongress / Trade fair and Congress
A+A 2023
Messe Düsseldorf
www.aplusa-online.com

25.10.23 » Online

Informationsveranstaltung
Dresdner Treffpunkt „Kollege Roboter – Mensch-Roboter Interaktion in der betrieblichen Praxis“
Bundesanstalt für Arbeitsschutz und Arbeitsmedizin
www.baua.de 🔎 Kollege Roboter

25.-27.10.23 » Dresden

Seminar
Grundlagen der Normungsarbeit im Arbeitsschutz
IAG/KAN
https://asp.veda.net/webgate_dguv_prod
🔎 570044

26.10.23 » Düsseldorf

Kongress
GfA-Herbstkongress 2023 „Nachhaltige Sicherheit und Gesundheit bei der Arbeit“
Gesellschaft für Arbeitswissenschaft (GfA)
www.gesellschaft-fuer-arbeitswissenschaft.de

02.11.23 » Berlin

Nationaler Kick-off der EU-OSHA-Kampagne 2023-25
Sicher und gesund arbeiten in Zeiten der Digitalisierung
BAuA/DGUV/EU-OSHA
www.baua.de 🔎 Nationaler Kick-off

13.11.23 – 18.01.24 » Dresden/Online

Seminar
Normungsarbeit im Arbeitsschutz weiterdenken – Aufbauseminar
IAG/KAN
https://asp.veda.net/webgate_dguv_prod 🔎 570139

15.11.23 » Online

Informationsveranstaltung
Dresdner Treffpunkt „Die neue europäische Maschinenverordnung“
Bundesanstalt für Arbeitsschutz und Arbeitsmedizin
www.baua.de 🔎 Maschinenverordnung

27.-28.11.23 » Bonn

Seminar
Maschinenanlagen/Technische Anlagen
MBT
www.maschinenbautage.eu/seminare/seminarmaschinenanlagen

29.11.-01.12.23 » Dresden

Seminar
Sicherer Einsatz von kollaborierenden Robotern
Institut für Arbeit und Gesundheit der DGUV (IAG)
https://asp.veda.net/webgate_dguv_prod
🔎 570164

04.-07.12.23 » Sankt Augustin

Seminar
Sicherheitstechnik von Maschinen
Institut für Arbeitsschutz der DGUV (IFA)
https://dguv.converia.de/frontend/index.php?sub=94

Zamówienie

www.kan.de/en » Publications » Orders (bezpłatnie)

Gefördert durch: Bundesministerium für Arbeit und Soziales aufgrund eines Beschlusses des Deutschen Bundestages

Impressum

Edytor
Verein zur Förderung der Arbeitssicherheit in Europa e.V. (VFA) przy wsparciu finansowym Federalnego Ministerstwa Pracy i Spraw Społecznych.

Redakcja
Komisja Ochrony Pracy i Normalizacji (KAN) - Sekretariat
Sonja Miesner, Michael Robert
Tel. +49 2241 231 3450 · www.kan.de · info@kan.de

Dyrekcja
Angela Janowitz, Alte Heerstr. 111, D – 53757 Sankt Augustin

Tłumaczenie
Ewa Marzodko

Wydanie kwartalnie, bezpłatnie

ISSN: 2702-4024 (Print) · 2702-4032 (Online)