DIGITALEUROPE

Transpozycja dyrektywy w sprawie bezpieczeństwa sieci i systemów informatycznych UE

Bruksela, 5 Lipiec 2016 r.

STRESZCZENIE

W dniu 21 kwietnia 2016 r. Rada Unii Europejskiej opublikowała ostateczną wersję dyrektywy w sprawie bezpieczeństwa sieci i systemów informatycznych. Chociaż dyrektywa ma zostać formalnie zatwierdzona przez Parlament Europejski latem, sam tekst został uzgodniony przez trzy najważniejsze instytucje europejskie i nie przewiduje się jego zmiany. Państwa członkowskie są zobowiązane do transpozycji dyrektywy do prawa krajowego w ciągu 21 miesięcy od czasu jej przyjęcia. Aby wesprzeć ten proces, w poniższym załączniku przedstawiamy wytyczne dotyczące najlepszych praktyk w zakresie wdrażania aspektów związanych z sektorem technologii i skutecznego uwzględnienia intencji autorów projektu.

Dyrektywa w sprawie bezpieczeństwa sieci i systemów informatycznych UE jest pierwszym ogólnoeuropejskim aktem ustawodawczym dotyczącym bezpieczeństwa cybernetycznego, którego głównymi celami są wzmocnienie organów odpowiedzialnych za bezpieczeństwo cybernetyczne na szczeblu krajowym, lepsza koordynacja między nimi i wprowadzenie wymogów bezpieczeństwa w kluczowych sektorach przemysłu.

Wszelkie krajowe przepisy wykonawcze powinny uwzględniać dwa główne cele dyrektywy: (1) zapewnienie wysokiego poziomu bezpieczeństwa cybernetycznego krajowej infrastruktury krytycznej; (2) ustanowienie skutecznego mechanizmu współpracy między państwami członkowskimi UE sprzyjającego temu celowi. Środki powinny zostać przeznaczone przede wszystkim na osiągnięcie tych dwóch ważnych celów.

W przypadku sektora technologii szczególne znaczenie mają przepisy dotyczące tzw. dostawców usług cyfrowych. W dyrektywie jasno określono, że między operatorami usług kluczowych a dostawcami usług cyfrowych występują podstawowe różnice. Dostawców usług cyfrowych nie uznaje się za infrastrukturę krytyczną. Zgodnie z przepisami incydentowi zakłócającemu usługi cyfrowe jest przypisany znacznie mniejszy poziom ryzyka dla bezpieczeństwa gospodarczego i publicznego danego kraju. Utrzymanie tego rozróżnienia ma kluczowe znaczenie dla skutecznego wykorzystania niewielkich zasobów organów, które będą odpowiedzialne za nadzorowanie i egzekwowanie przepisów.

W konsekwencji zalecamy zwrócenie szczególnej uwagi na zamierzony zakres przedmiotowy usług oraz wezwanie decydentów do nieuwzględniania w przepisach krajowych sektorów innych niż określone jako dostawcy usług cyfrowych lub operatorzy usług kluczowych.

W kwestii jurysdykcji dostawcy usług cyfrowych powinni podlegać prawu obowiązującemu w kraju swojej głównej jednostki organizacyjnej, nawet w przypadkach zaangażowania właściwych organów z więcej niż jednego kraju. W kwestii kontroli właściwe organy powinny stosować podejście ex-post w miejsce narzucania ogólnego obowiązku nadzorowania dostawców usług cyfrowych. Ponadto powinny skoncentrować się na wynikach i utrzymać rozróżnienie między operatorami usług kluczowych a dostawcami usług cyfrowych, powstrzymując się od nakładania na tych drugich wymogów nieprzewidzianych w dyrektywie, takich jak audyt i wiążące instrukcje.

DIGITALEUROPE
Rue de la Science, 14 - 1040 Brussels [Belgia]
Tel. +32 (0) 2 609 53 10 Faks +32 (0) 2 431 04 89
www.digitaleurope.org | info@digitaleurope.org | @DIGITALEUROPE
Organizacja wpisana do rejestru Komisji służącego przejrzystości pod numerem: 64270747023-20

Środki bezpieczeństwa dotyczące dostawców usług cyfrowych powinny różnić się od środków przewidzianych dla operatorów usług kluczowych, mając na uwadze, że zgodnie z dyrektywą podlegają oni zdecydowanie mniejszemu ryzyku dla bezpieczeństwa. Decydenci powinni mieć świadomość celu harmonizacji tych usług, uznawać istniejące międzynarodowe normy obowiązujące w sektorze, unikać nakładania uprawnień technologicznych i przestrzegać przewidzianego w dyrektywie prawa dostawców usług cyfrowych do określania środków bezpieczeństwa najbardziej odpowiednich dla ich systemów. Zgłaszanie incydentów również należy możliwie jak najbardziej zharmonizować na szczeblu europejskim. Powinno ono koncentrować się na incydentach mających wpływ na ciągłość usługi, odbywać się w poszanowaniu elastyczności w kwestii czasu zgłaszania i stwarzać godne zaufania środowisko, które zachęca do wymiany informacji bez narażania zgłaszającego na większą odpowiedzialność.

Środki nałożone na operatorów usług kluczowych będą miały również wpływ na inne sektory i, podobnie jak środki bezpieczeństwa oraz zgłaszanie incydentów, znajdą odzwierciedlenie w postanowieniach umownych. Dotyczy to w szczególności usług w chmurze. W konsekwencji dostawcy usług cyfrowych mogą pośrednio podlegać przepisom krajowym swoich klientów, stąd duże zainteresowanie możliwością stosowania do tych usług środków bezpieczeństwa o międzynarodowym uznaniu. Proponujemy również możliwie jak największy stopień koordynacji i synergii między wymogami dotyczącymi zgłaszania, zarówno wobec operatorów usług kluczowych, jak i dostawców usług cyfrowych , mając na uwadze, że ci ostatni mogą być przedmiotem podwójnego zgłoszenia.

Dyrektywa stawia sobie za cel osiągnięcie wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych dla poprawy funkcjonowania rynku wewnętrznego. Aby osiągnąć ten ambitny cel, organy krajowe odpowiedzialne za transpozycję powinny przyjąć międzynarodowe, zharmonizowane podejście oparte na ocenie ryzyka, które zapewnia podmiotom z sektora prywatnego elastyczność w dostosowywaniu się do nieustannie zmieniającego się charakteru zagrożeń, umożliwia organom odpowiedzialnym za bezpieczeństwo cybernetyczne skierowanie ograniczonych zasobów na najbardziej kluczowe wyzwania i uznaje potrzebę znalezienia globalnego rozwiązania dla problemu o charakterze ponadgranicznym. Mamy nadzieję, że niniejsze wytyczne okażą się przydatne w dążeniu do tego celu i z chęcią odpowiemy na wszelkie pytania.

Załącznik: Wytyczne dotyczące najlepszych praktyk w zakresie wdrażania dyrektywy w sprawie bezpieczeństwa sieci i systemów informatycznych

1. Dostawcy usług cyfrowych

a) Zakres

- Dyrektywa stanowi, że internetowe platformy handlowe, wyszukiwarki internetowe i usługi przetwarzania w chmurze należy uznać za dostawców usług cyfrowych i tym samym zostają one objęte dyrektywą. Ponieważ dyrektywa przewiduje minimalny poziom harmonizacji (art. 2), należy utrzymać spójność w całej UE, co oznacza, że w ustawodawstwie krajowym państwa członkowskie nie powinny nakładać wymogów bezpieczeństwa na sektory inne niż określone jako dostawcy usług cyfrowych lub operatorzy usług kluczowych, o których mowa w art. 3.

- Dyrektywa wyraźnie stanowi, że producenci sprzętu i twórcy oprogramowania nie są dostawcami usług cyfrowych ani operatorami usług kluczowych, co oznacza, że nie powinni podlegać krajowym przepisom wdrażającym dyrektywę (motyw 50).

- W dyrektywie wyraźnie wyłączono z zakresu internetowych platform handlowych usługi internetowe spełniające wyłącznie funkcję pośredniczącą wobec usług stron trzecich w przypadku ostatecznego zawarcia umowy sprzedaży lub świadczenia usług (np. witryny oferujące porównywanie cen) (motyw 15).

- Definicja wyszukiwarki internetowej nie powinna obejmować funkcji wyszukiwania, które ogranicza się do wyszukiwania treści na konkretnej stronie internetowej, nawet w przypadku korzystania z usług dostawcy zewnętrznego (motyw 16).

- Przewidziana w dyrektywie definicja usługi przetwarzania w chmurze zależy od zasobów komputerowych udostępnianych przez różnych użytkowników (art. 4 pkt. 19 oraz motyw 17). Mając na uwadze, że prywatne usługi w chmurze (w przeciwieństwie do publicznych usług w chmurze) są przeznaczone dla pojedynczej organizacji, również nie powinny być one objęte definicją dostawców usług cyfrowych.

- W dyrektywie podkreślono, że między operatorami usług kluczowych a dostawcami usług cyfrowych występują podstawowe różnice i z tego powodu dostawcy usług cyfrowych podlegają różnym przepisom (motyw 57). Takie rozróżnienie należy utrzymać podczas wdrażania dyrektywy.

b) Jurysdykcja i kontrola

- Jurysdykcję w odniesieniu do dostawców usług cyfrowych należy powierzyć tylko jednemu państwu członkowskiemu, w którym dany dostawca usług cyfrowych ma główną jednostkę organizacyjną w UE, która co do zasady odpowiada miejscu, gdzie znajduje się siedziba zarządu danego dostawcy w UE (art. 18 ust. 1 oraz motyw 64). Uważamy, że dostawcy usług internetowych powinni sami dokonać takiego ustalenia, a decyzja powinna podlegać przeglądowi tylko wtedy, gdy właściwe organy nie osiągną porozumienia w przypadku działań związanych z kontrolą ex-post.

- W przypadku, gdy dostawcy usług cyfrowych dysponują sieciami i systemami informacji w krajach innych niż siedziba ich głównej jednostki organizacyjnej, art. 17 ust. 3 przewiduje współpracę właściwych organów. Jednakże z punktu widzenia dostawców usług cyfrowych istotne jest to, żeby zastosowanie miało prawo kraju, w którym znajduje się ich główna jednostka organizacyjna oraz żeby ponosili odpowiedzialność wyłącznie przed właściwym organem w obrębie tej jurysdykcji, który powinien występować jako strona dialogu.

- W dyrektywie podkreślono, że dostawcy usług cyfrowych podlegają reaktywnym działaniom nadzorczym ex-post, co oznacza, że właściwe organy nie mają ogólnego obowiązku nadzorowania dostawców usług cyfrowych i powinny podejmować działania wyłącznie po otrzymaniu dowodu (art. 17 ust. 1 oraz motyw 60). Postanowień tych należy przestrzegać podczas wdrażania dyrektywy.

- W przeciwieństwie do operatorów usług kluczowych dostawcy usług cyfrowych mogą wnioskować wyłącznie o informacje i domagać się wyeliminowania przypadków niespełnienia wymogów. W dyrektywie wyraźnie przewidziano, że organy nie mają uprawnień audytowych i nie mogą wydawać wiążących instrukcji. Postanowienia te powinny być również przestrzegane na szczeblu krajowym.

c) Dodatkowe wymogi

- Wymogi dotyczące bezpieczeństwa i zgłaszania nałożone na dostawców usług cyfrowych podlegają maksymalnej harmonizacji (art. 16 ust. 10). Należy przewidzieć zastosowanie tego artykułu w odniesieniu do produktów, usług i rozwiązań, które tworzą sieci i systemy informatyczne. W konsekwencji dodatkowe przepisy, takie jak testowanie produktu, nie powinny być wymagane, jeżeli produkty i usługi są wykorzystywane w tym kontekście.

d) Środki i normy bezpieczeństwa

- Środki bezpieczeństwa dotyczące dostawców usług cyfrowych powinny być mniej rygorystyczne niż w przypadku operatorów usług kluczowych. Dostawcom usług cyfrowych należy pozostawić swobodę podejmowania środków, które uznają za odpowiednie do zarządzania ryzykami, na jakie może być narażone bezpieczeństwo ich sieci i systemów informatycznych (motyw 49).

- Środki bezpieczeństwa powinny być ukierunkowane na proces i zarządzanie ryzykiem. Nie powinny wiązać się z koniecznością projektowania, opracowywania lub produkowania produktów technologii teleinformatycznych w żaden określony sposób (motyw 51).

- W dyrektywie podkreślono, że państwa członkowskie nie powinny nakładać żadnych dodatkowych wymogów dotyczących bezpieczeństwa na dostawców usług cyfrowych (art. 16 ust. 10).

- Niemniej jednak oczekujemy wytycznych od różnych podmiotów. Państwa członkowskie zagwarantują przyjęcie środków przewidzianych w dyrektywie (art. 16 ust. 1), mogą zachęcać do stosowania norm w celu ich wdrażania (art. 19 ust.1) i omawiać normy z europejskimi organizacjami normalizacyjnymi w ramach grupy współpracy (art. 11 ust. 3 lit. h). ENISA zapewni doradztwo w kwestii odpowiednich norm (art. 19 ust. 2), a Komisja Europejska jest odpowiedzialna za przyjęcie aktów wykonawczych dotyczących środków bezpieczeństwa (art. 16 ust. 8).

- Mając na uwadze poziom złożoności harmonizacji i płynących z niej korzyści, zalecamy, aby w ramach procesów krajowych uwzględniać akty wykonawcze w zakresie uzgadniania odpowiednich środków, które należy sfinalizować w ciągu jednego roku od przyjęcia dyrektywy. Same akty wykonawcze nie powinny naruszać możliwości określenia przez dostawców usług cyfrowych środków bezpieczeństwa najbardziej odpowiednich dla ich systemów.

- Artykuł w sprawie norm umożliwia powoływanie się na normy europejskie lub normy uznane międzynarodowo (art. 19 ust. 1). Mając na uwadze dojrzałość norm międzynarodowych obowiązujących w tej dziedzinie, zalecamy, aby tam, gdzie istnieją odpowiednie normy, uznać certyfikację według jednej z nich (np. ISO 27001) jako wystarczającą do spełniania wymogów.

- W każdym przypadku certyfikacja nie powinna być obowiązkowa, lecz fakultatywna. W art. 19 podkreślono, że należy jedynie „zachęcać" do stosowania norm, „nie narzucając ani nie faworyzując wykorzystywania określonego rodzaju technologii".

e) Zgłaszanie incydentów dotyczących bezpieczeństwa

- Podobnie jak w przypadku środków bezpieczeństwa, różne strony biorą udział w mechanizmie zgłaszania incydentów przewidzianym w dyrektywie w sprawie bezpieczeństwa sieci i systemów informatycznych. Państwa członkowskie muszą zagwarantować zgłaszanie przez dostawców usług cyfrowych tych incydentów, które mają wpływ na świadczenie usługi (co mieści się w zakresie dyrektywy) (art. 16 ust. 3), grupa współpracy odpowiada za omówienie zasad zgłaszania (art. 11 ust. 3 lit. m), a Komisja za przyjęcie aktów wykonawczych (art. 16 ust. 8 i 9).

- Również w tym przypadku zalecamy, aby w procesie transpozycji na szczeblu krajowym uwzględnić te kwestie w aktach wykonawczych, wśród których akt wykonawczy w sprawie progów wymagających zgłoszenia należy przyjąć w ciągu jednego roku od sfinalizowania dyrektywy.

- Co się tyczy rodzajów incydentów, jakie należy zgłaszać, dostawcy usług cyfrowych mają obowiązek zgłaszać „wszelkie incydenty mające istotny wpływ na świadczenie [ich] usługi" (art. 16 ust.3). Jeżeli chodzi o wdrażanie równoważnych przepisów w odniesieniu do operatorów usług telekomunikacyjnych na mocy art. 13a dyrektywy ramowej, uważamy, że należy je interpretować w taki sposób, aby położyć nacisk na ciągłość (lub dostępność) świadczonych usług. Innymi słowy awarie, które osiągną określony pułap (ustalony w aktach wykonawczych), powinny być zgłaszane jako inny rodzaj incydentów dotyczących bezpieczeństwa. Zaletą takiego podejścia jest skoncentrowanie się na incydentach, które mają największy wpływ na gospodarkę lub społeczeństwo, a jednocześnie minimalizują (chociaż nie całkowicie eliminują) zgłaszanie awarii objętych równocześnie obowiązkiem zgłaszania naruszenia danych osobowych wynikającym z ogólnego rozporządzenia o ochronie danych.

- Ponadto obowiązek zgłaszania spoczywający na operatorach usług kluczowych przewiduje, że operatorzy ci zgłaszają „incydenty mające istotny wpływ na ciągłość świadczonych przez nich usług kluczowych", co oznacza, że ponownie położono wyraźny nacisk na ciągłość (lub dostępność) usługi. Współprawodawcy uzgodnili, że obowiązki spoczywające na dostawcach usług cyfrowych powinny być mniej rygorystyczne niż obowiązki spoczywające na operatorach usług kluczowych (zob.motyw 49). Oznacza to, że obowiązek zgłaszania incydentów spoczywający na dostawcach usług cyfrowych w ramach

bezpieczeństwa sieci i systemów informatycznych nie powinien być szerszy niż obowiązki operatorów usług kluczowych, lecz powinien być jeszcze bardziej zawężony pod względem progów. Jest to jeszcze jeden wyraźny sygnał, że zgłaszanie incydentów przez dostawców usług cyfrowych powinno ograniczać się do incydentów, które osiągają konkretny próg i **mają wpływ na ciągłość/dostępność usługi**, oraz nie dotyczy incydentów związanych z integralnością lub poufnością danych, które w znacznej mierze już są objęte obowiązkiem zgłaszania przewidzianym w ogólnym rozporządzeniu o ochronie danych i rozporządzeniu w sprawie identyfikacji elektronicznej (eIDAS).

- Jeżeli chodzi o czas zgłoszenia, uznajemy elastyczność wynikającą z zapisu o zgłaszaniu „bez zbędnej zwłoki" (art. 16 ust. 3). Implementacja nie powinna nakładać sztywnych terminów, ponieważ incydenty różnią się znacznie od siebie pod względem złożoności. Jednolite terminy zgłaszania doprowadziłyby do nieprawidłowości zgłaszania w przypadku, gdy pierwotny zakres systemów byłby niejasny i miałyby wpływ na zdolność specjalistów zajmujących się reagowaniem na incydenty do ustalenia priorytetu reakcji na dany incydent.

- Jak wynika z rozmów prowadzonych na ten temat, incydenty dotyczące bezpieczeństwa, które powinny być zgłaszane na mocy dyrektywy, mogą również wymagać zgłoszenia na podstawie ustawy o ochronie danych w zależności od tego, czy nastąpiło naruszenie danych osobowych. Oznacza to nie tylko zgłaszanie tego samego incydentu różnym organom, lecz może nawet oznaczać, że organy te będą pochodzić z różnych państw członkowskich w zależności od tego, która jurysdykcja znajdzie zastosowanie w sprawie dostawców usług cyfrowych na mocy tych dwóch aktów prawnych. Zalecamy, aby państwa członkowskie uznały potrzebę wprowadzenia jednolitego mechanizmu zgłaszania incydentów i dążyły do utworzenia kanałów komunikacji służących wymianie odpowiednich informacji między sobą, bez uszczerbku dla poufności zawodowej.

- Właściwe organy powinny uwzględniać kwestie związane z reputacją i działalnością handlową dostawców usług cyfrowych przed podaniem informacji o incydencie do publicznej wiadomości. Co ważniejsze, ujawnienie incydentu mogłoby zwiększyć ryzyko dla bezpieczeństwa. Z tego względu przed ujawnieniem jakichkolwiek informacji ważna jest koordynacja z podmiotami, o których mowa.

- W dyrektywie podkreślono, że informacje uznawane za poufne powinny być traktowane jako takie (motywy 41, 59, art. 1 ust. 5).

- W art. 16 ust. 3 podkreślono, że zgłaszanie incydentów nie może narażać strony zgłaszającej na zwiększoną odpowiedzialność.

2. Operatorzy usług kluczowych

a) Odzwierciedlenie w środkach bezpieczeństwa

- Dostawcy usług cyfrowych, których klientami są operatorzy usług kluczowych, będą podlegać odpowiednim środkom bezpieczeństwa wynikającym z obowiązków statusowych dotyczących operatorów usług kluczowych, co znajdzie odzwierciedlenie w negocjacjach dotyczących umowy (art. 14 ust. 1). W związku z tym mogą pośrednio podlegać prawu krajowemu swoich klientów bez względu na prawo obowiązujące w kraju ich europejskiej siedziby.

- W związku z tym pożądane są wysiłki zmierzające do harmonizacji środków bezpieczeństwa dotyczących operatorów usług kluczowych. Ponieważ państwa członkowskie mają prawo nakładania na operatorów usług kluczowych bardziej rygorystycznych obowiązków niż obowiązki wynikające z dyrektywy (art. 3), zalecamy, aby się od tego powstrzymać, oraz zachęcamy państwa członkowskie do działań zmierzających w kierunku harmonizacji. Można ją osiągnąć, unikając dodatkowych środków w ramach transpozycji na szczeblu krajowym oraz dążąc do ustalenia odpowiednich środków bezpieczeństwa w ramach grupy współpracy zamiast skupiania się na procesach krajowych.

- Wymogi dotyczące bezpieczeństwa powinny opierać się w jak największym zakresie na normach międzynarodowych (takich jak z grupy ISO 27000) i uznawanych najlepszych praktykach w dziedzinie bezpieczeństwa.

- Środki bezpieczeństwa nałożone na operatorów usług kluczowych nie powinny w żadnym razie wiązać się z koniecznością projektowania, opracowywania lub produkowania produktów technologii teleinformatycznych w określony sposób (motyw 51).

b) Odzwierciedlenie w zgłaszaniu incydentów dotyczących bezpieczeństwa

- Operatorzy usług kluczowych mają obowiązek zgłaszania incydentów związanych z dostawcami usług cyfrowych, z którymi łączy ich umowa, jeżeli mają one wpływ na ciągłość ich kluczowych usług (art. 16 ust. 5). Dostawcy usług cyfrowychmają zatem umowny obowiązek zgłaszania operatorowi usług kluczowych incydentów związanych z bezpieczeństwem, które mogą mieć na niego wpływ.

- Uznajemy elastyczność czasu zgłaszania incydentów przez operatorów usług kluczowych, która znalazła wyraz z sformułowaniu „bez zbędnej zwłoki ” (art. 14 ust. 3). W procesie transpozycji na szczeblu krajowym nie należy wprowadzać specjalnych terminów, a w jakimkolwiek przypadku, gdy operatorzy usług kluczowych muszą uzasadnić czas poświęcony na zgłoszenie, okres, który podlega ocenie, powinien zacząć biec od momentu, w którym operator usług kluczowych został powiadomiony o incydencie, a nie od momentu, w którym dostawca usług cyfrowych został o nim powiadomiony. .

- W art. 14 ust. 7 przewiduje się, że grupa współpracy sporządza wytyczne dotyczące okoliczności zgłaszania incydentów w przeciwieństwie do harmonizującej roli zgłoszeń dokonywanych przez dostawców usług cyfrowych. Mając na uwadze podwójny wymóg zgłaszania spoczywający na dostawcach usług cyfrowych, istotne jest, aby odpowiednie wymogi w zakresie zgłaszania nie były sprzeczne i zostały jak najlepiej dostosowane. Zatem proces powinien zostać poddany kontroli pod kątem tego wymogu. Ponadto wymogi dotyczące dokonywania zgłoszeń przez dostawców usług cyfrowych powinny być zgodne z obowiązkiem zachowania poufności wobec klientów operatora usług kluczowych i nie powinny nakazywać przekazywania poufnych informacji zawodowych.

O DIGITALEUROPE

DIGITALEUROPE reprezentuje sektor technologii cyfrowych w Europie. Wśród naszych członków znajdują się największe światowe firmy telekomunikacyjne i przedsiębiorstwa z branży elektroniki użytkowej oraz stowarzyszenia krajowe z każdej części Europy. DIGITALEUROPE dąży do tego, aby przedsiębiorstwa europejskie i obywatele europejscy mogli w pełni korzystać z technologii cyfrowych, i stawia sobie za cel wzrost rynku Europy, przyciąganie i utrzymanie najlepszych światowych przedsiębiorstw z sektora technologii cyfrowych.

DIGITALEUROPE zapewnia udział przedstawicieli sektora w opracowywaniu i wdrażaniu unijnych strategii politycznych. DIGITALEUROPE liczy 62 członków korporacyjnych i 37 krajowych stowarzyszeń handlowych z całej Europy. Na naszej witrynie można znaleźć aktualne informacje o naszej działalności: http://www.digitaleurope.org

CZŁONKOWIE DIGITALEUROPE

Członkowie korporacyjni

Airbus, Amazon Web Services, AMD, Apple, BlackBerry, Bose, Brother, CA Technologies, Canon, Cisco, Dell, Epson, Ericsson, Fujitsu, Google, Hewlett Packard Enterprise, Hitachi, HP Inc., Huawei, IBM, Ingram Micro, Intel, iQor, JVC Kenwood Group, Konica Minolta, Kyocera, Lenovo, Lexmark, LG Electronics, Loewe, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, NEC, Nokia, Nvidia Ltd., Océ, Oki, Oracle, Panasonic Europe, Philips, Pioneer, Qualcomm, Ricoh Europe PLC, Samsung, SAP, SAS, Schneider Electric IT Corporation, Sharp Electronics, Siemens, Sony, Swatch Group, Technicolor, Texas Instruments, Toshiba, TP Vision, VMware, Western Digital, Xerox, Zebra Technologies, ZTE Corporation.

Krajowe stowarzyszenia handlowe

Austria: IOÖ
Belgia: AGORIA
Białoruś: INFOPARK
Bułgaria: BAIT
Cypr: CITEA
Dania: DI Digital, IT-BRANCHEN
Estonia: ITL
Finlandia: FFTI
Francja: AFNUM, Force Numérique, Tech in France
Grecja: SEPE
Hiszpania: AMETIC
Holandia: Nederland ICT, FIAR
Irlandia: ICT IRELAND
Litwa: INFOBALT
Niemcy: BITKOM, ZVEI
Polska: KIGEIT, PIIT, ZIPSEE
Portugalia: AGEFE
Rumunia: ANIS, APDETIC
Słowacja: ITAS
Słowenia: GZS
Szwajcaria: SWICO
Szwecja: Foreningen Teknikföretagen i Sverige, IT&Telekomföretagen
Turcja: Digital Turkey Platform, ECID
Ukraina: IT UKRAINE
Węgry: IVSZ
Wielka Brytania: techUK
Włochy: ANITEC