



Dyrektywa NIS2: Cyberbezpieczeństwo w UE

Zrozumienie i wdrażanie wymogów NIS2

Spis treści

1.	Czym jest NIS2?	2
2.	Co nowego w NIS2?	3
2.1.	NIS2 wpływa na więcej sektorów i organizacji	3
2.2.	Niezgodność jest kosztowna	3
2.3.	Dodatkowe środki w ramach NIS2	3
2.4.	Odpowiedzialność zarządzających za naruszenia	4
3.	Kogo obejmuje NIS2?	5
4.	Działania obowiązkowe	7
4.1.	Rejestr podmiotów ważnych i kluczowych	7
4.2.	Zgłaszanie incydentów bezpieczeństwa	8
5.	Cel NIS2: zarządzanie ryzykiem	9
	Jakie środki zarządzania ryzykiem reguluje dyrektywa NIS2?	10
6.	Z baramundi do zgodności z NIS2	11
6.	Kolejne kroki w kierunku zgodności z NIS2	12

1. Czym jest NIS2?

Na całym świecie, w tym w UE, rośnie liczba i skala zagrożeń cyberbezpieczeństwa. Szczególnie narażona jest infrastruktura krytyczna zasadnicza do sprawnego funkcjonowania społeczeństwa. Przykładowo, cyberatak powodujący awarię sieci energetycznej może doprowadzić do zatrzymania najważniejszych usług, takich jak szpitale, systemy łączności i stacje uzdatniania wody.

Chociaż klasyfikacja infrastruktury krytycznej różni się w krajach UE, państwa członkowskie pracują nad zwiększeniem cyberbezpieczeństwa w kluczowych sektorach poprzez ustalenie jednolitych standardów. Służyła temu dyrektywa z 2016 r. w sprawie bezpieczeństwa sieci i informacji (NIS). NIS wymagała od organizacji infrastruktury krytycznej przestrzegania zestawu norm dotyczących bezpieczeństwa sieci i systemów. Dyrektywa NIS określiła wspólne zasady i minimalne wymagania, ale pozostawiła ich wdrożenie w gestii poszczególnych państw członkowskich.

W styczniu 2023 r. NIS2 zastąpiła NIS. Znowelizowana wersja tej dyrektywy zwiększa wymogi bezpieczeństwa dla podmiotów infrastruktury krytycznej i znacznie rozszerza liczbę organizacji jej podlegającym.¹

Większość objętych dyrektywą NIS2 firm będzie musiała przeznaczyć dodatkowe zasoby na osiągnięcie i utrzymanie zgodności z jej wymogami, począwszy od narzędzi i praktyk mających na celu poprawę przejrzystości i bezpieczeństwa infrastruktury IT, a skończywszy na konkretnych środkach [Cel NIS2](#): zarządzanie ryzykiem. Ponadto, jednym z najważniejszych nowych aspektów NIS2 jest fakt, że regulacje te dotyczą większej liczby osób w każdej organizacji niż tylko specjalistów IT. Różni managerowie wyższego szczebla, kadra kierownicza, tj. szefowie bezpieczeństwa informacji (CISO) oraz dział, w tym operacyjny i finansowy, będą teraz wspólnie odpowiadać za zapewnienie cyberbezpieczeństwa. Dzięki temu ochrona sieci i informacji staje się coraz bardziej strategiczną i biznesową kwestią kultury organizacyjnej. Rozwiązania służące do ujednoliconego zarządzania punktami końcowymi mogą zapewnić cenne wsparcie w spełnianiu nowych wymagań poprzez zautomatyzowanie wielu rutynowych zadań związanych z bezpieczeństwem, szczególnie w przypadku organizacji z coraz bardziej złożoną infrastrukturą informatyczną, w których brakuje wykwalifikowanych pracowników.

¹ Treść całej dyrektywy można znaleźć pod adresem: <https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32022L2555>.

2. Co nowego w NIS2?

NIS2 znacząco wzmacnia i uzupełnia regulacje zawarte w poprzedniej wersji dyrektywy NIS z 2016 r., w tym m.in.:

- obejmuje więcej sektorów, klasyfikując je jako „kluczowe” oraz „istotne” ze względu na ich znaczenie,
- wyznacza wyższe kary za nieprzestrzeganie przepisów i zwiększa znaczenie nadzoru,
- angażuje i zwiększa odpowiedzialność kierownictwa wyższego szczebla za zgodność z przepisami,
- zwiększa obowiązki sprawozdawcze,
- określa obowiązkowe środki bezpieczeństwa, które firmy muszą regularnie przeprowadzać i dokumentować, ze zwiększonym naciskiem na zarządzanie ryzykiem.

2.1. NIS2 wpływa na więcej sektorów i organizacji

Wymagane środki cyberbezpieczeństwa dotyczą większej liczby branż. W efekcie nowa dyrektywa ma wpływ na organizacje w 11 sektorach „kluczowych” i siedmiu „istotnych”. Klasyfikacja firmy jako kluczowej lub istotnej zależy od tego, do którego sektora została przypisana i od jej wielkości (patrz rozdział 4).

2.2. Niezgodność jest kosztowna

Przedsiębiorstwa są narażone na znaczne grzywny za naruszenie przepisów NIS2. Organizacjom z istotnych sektorów, w tym produkcji żywności, usług cyfrowych, chemikaliów i produkcji, grożą grzywny w wysokości do 7 milionów euro lub 1,4 proc. ich rocznych przychodów. Kluczowe organizacje w sektorach takich jak transport, finanse, energia i infrastruktura cyfrowa mogą zostać ukarane grzywną w wysokości do 10 milionów euro lub 2 proc. ich rocznych przychodów. Rażące naruszenia mogą skutkować grzywnami w wysokości do 20 milionów euro lub 4 proc. globalnego rocznego przychodu. Osoby naruszające przepisy mogą również podlegać nadzorowi rządowemu w celu zapewnienia zgodności, w tym kontroli reaktywnej po incydencie w istotnych spółkach oraz kontroli proaktywnej z ciągłym monitorowaniem najistotniejszych organizacji.

2.3. Dodatkowe środki w ramach NIS2

Firmy podlegające NIS2 będą również musiały wdrożyć surowsze i szerzej obejmujące środki ochrony IT, ze szczególnym naciskiem na zarządzanie ryzykiem i bezpieczeństwo łańcucha dostaw. Wśród innych wymogów znajdują się regularne testy zabezpieczeń, zgłaszanie incydentów bezpieczeństwa oraz wdrożenie aktywnych środków ochronnych sieci i systemów. W zależności od wagi incydentów, organizacje będą zobowiązane do ich zgłaszania w swoich krajach lub, w razie potrzeby, w całej UE.

2.4. Odpowiedzialność zarządzających za naruszenia

Wśród najważniejszych elementów NIS2 znajdują się środki mające na celu pociągnięcie do osobistej odpowiedzialności managerów wyższego szczebla i kadry zarządzającej za incydenty bezpieczeństwa wynikające z rażącego zaniedbania lub nieprzestrzegania przepisów. Managerowie w organizacjach objętych NIS2 mają obowiązek monitorować wdrażanie środków cyberbezpieczeństwa, podczas gdy dyrektorzy i inni członkowie zarządu muszą przechodzić regularne szkolenia z zarządzania związanego z cyberbezpieczeństwem oraz posiadać wiedzę i umiejętności niezbędne do utrzymania przez ich organizacje zgodności z wymogami dyrektywy i cyberodporności.

Infobox: ochrona przed cyberzagrożeniami – wymogi NIS2 w skrócie:

- Wytyczne (polityki) dotyczące zarządzania ryzykiem i bezpieczeństwa informacji
- Zarządzanie incydentami, by zapobiegać, wykrywać i rozwiązywać incydenty bezpieczeństwa
- Ciągłość działania oparta na tworzeniu kopii zapasowych, odzyskiwaniu danych po awarii i zarządzaniu kryzysowym
- Bezpieczeństwo łańcucha dostaw i środki na rzecz bezpiecznego zakupu systemów informatycznych i sieciowych
- Specyfikacje analizy cyberryzyka i zarządzania nim
- Specyfikacje dotyczące szyfrowania (kryptografii)
- Kontrola dostępu z użyciem uwierzytelniania wieloskładnikowego i jednokrotnego logowania
- Środki bezpieczeństwa w zakresie komunikacji głosowej, wideo oraz tekstowej

3. Kogo obejmuje NIS2?

NIS2 znacznie zwiększa liczbę sektorów i organizacji, podlegających rozszerzonym wymogom cyberbezpieczeństwa. „Kluczowe podmioty” uznane za niezbędne do funkcjonowania gospodarki i społeczeństwa obejmują organizacje z branży energetycznej, transportowej, bankowej, rynków finansowych, zdrowia, wody pitnej, ścieków, infrastruktury cyfrowej, zarządzania usługami informacyjno-komunikacyjnymi, administracji publicznej i lotnictwa. „Istotne podmioty” to organizacje, które działają w sektorach wysokiego ryzyka, ale mogą mieć mniej infrastruktury krytycznej niż podmioty kluczowe. Obejmują one organizacje zajmujące się usługami pocztowymi i kurierskimi, gospodarką odpadami, wytwarzaniem produktów o znaczeniu krytycznym, takich jak środki farmaceutyczne, wyroby medyczne i artykuły przemysłowe, produkcją i dystrybucją chemikaliów, jak również produkcją, przetwarzaniem i dostawami żywności, usługami cyfrowymi oraz badaniami i edukacją.

Wielkość firmy wpływa również na jej klasyfikację jako „kluczowej” lub „istotnej”. Kluczowe organizacje obejmują średnie i duże przedsiębiorstwa zatrudniające 50 lub więcej pracowników albo o rocznych obrotach przekraczających 10 milionów euro. Obowiązkowi NIS2 podlegają jednak niektóre spółki zatrudniające mniej niż 50 pracowników lub mające obroty poniżej 10 mln euro, jeśli działają w sektorach uznanych za krytyczne dla bezpieczeństwa na poziomie krajowym i unijnym. Do istotnych podmiotów zalicza się zazwyczaj organizacje zatrudniające co najmniej 250 pracowników i osiągające roczny obrót przekraczający 50 milionów euro lub sumę bilansową przekraczającą 43 miliony euro. Ostateczna klasyfikacja zależy od implementacji dyrektywy w poszczególnych krajach.

Niezależnie od sektora lub wielkości, niektóre firmy, których dotyczy NIS2, przeoczą fakt, że dyrektywa ta obejmuje również łańcuchy dostaw. Oznacza to, że przedsiębiorstwa, które mają wśród swoich klientów organizacje podlegające NIS2, również będą musiały także dostosować się do jej wymogów.

Szacuje się, że nowe przepisy będą miały wpływ dodatkowo na ponad 100 000 firm w Europie. Kod NACE może być wykorzystany do sprawdzenia, czy nowe przepisy obejmują daną organizację² i jakie wymogi jej dotyczą. Na mocy dyrektywy NIS2 kierownictwo każdej organizacji musi przeprowadzić taką analizę wpływu do października 2024 r., by zapewnić zgodność z przepisami.

² Dodatkowe informacje na temat kodów NACE znajdują się na stronie: https://ec.europa.eu/competition/mergers/cases/index/nace_all.html.

Spełnienie dwóch z trzech kryteriów wielkości firmy:

Firma może zostać sklasyfikowana w jednej z klas MŚP, jeśli osiągnie liczbę zatrudnionych (50 pełnoetatowych pracowników (FTE)) i jeden z dwóch wskaźników finansowych.

Kategoria przedsiębiorstwa	FTE (jednostki pracy rocznie)	Roczny obrót	Bilans roczny
Średnie	≤ 250	≤ 50 mln EUR	≤ 43 mln EUR
Małe	≤ 50	≤ 10 mln EUR	≤ 10 mln EUR
Mikro	≤ 10	≤ 2 mln EUR	≤ 2 mln EUR

Przykład:

Niezależne prawnie przedsiębiorstwo z 49 etatami, rocznym obrotem wynoszącym 11 milionów euro oraz sumą aktywów wynoszącą 9 milionów euro może zostać sklasyfikowane jako małe przedsiębiorstwo, ponieważ zatrudnia mniej niż 60 pracowników i spełnia jedno z dwóch kryteriów finansowych. Gdyby firma wzrosła do 49 etatów, 11 milionów euro rocznego obrotu i 10 milionów euro łącznych aktywów, zostałaby uznana za średnie przedsiębiorstwo, objęte wymogami NIS2.

4. Działania obowiązkowe

NIS2 nakłada na przedsiębiorstwa dwa obowiązki sprawozdawcze. Pierwszym z nich jest wpis do rejestru podmiotów kluczowych i ważnych (w Polsce prowadzonego przez Ministra Cyfryzacji) a drugim – zgłaszanie incydentów bezpieczeństwa. Ten obowiązek w razie konieczności należy realizować bezzwłocznie.

4.1. Rejestr podmiotów ważnych i kluczowych

Podmioty objęte przepisami muszą dostarczyć szereg informacji do odpowiedniego organu w każdym kraju nie później niż trzy miesiące po ich początkowej lub odnowionej klasyfikacji NIS2. Są to: nazwa firmy, forma prawna, numer w rejestrze spółek (KRS), adres, dane kontaktowe (w tym e-mail, telefon, zakresy firmowych adresów IP), właściwy sektor lub podsektor oraz lista państw członkowskich UE, w których firma prowadzi działalność. Zmiany tych informacji muszą być również bezzwłocznie zgłaszane. Brak rejestracji lub rejestracja po terminie, a także opóźnienie w zgłoszeniu zmian są uważane za wykroczenia administracyjne w większości państw członkowskich.

4.2. Zgłaszanie incydentów bezpieczeństwa

Firmy objęte przepisami NIS2 są zobowiązane do bezzwłocznego powiadomienia odpowiedniego organu o „poważnym incydencie bezpieczeństwa”. Poważny incydent to taki, który spowodował lub mógłby spowodować istotne zakłócenia operacyjne lub straty finansowe narażonej organizacji bądź taki, który wpłynął lub może wpłynąć na inne osoby fizyczne czy prawne, powodując znaczne szkody majątkowe i niemajątkowe.

Obowiązki sprawozdawcze są wdrażane na poziomie krajowym w różny sposób. Organizacje w Polsce podlegają następującym wymogom:

- Firma musi bezzwłocznie – najpóźniej w ciągu 24 godzin od wykrycia – zgłosić poważny incydent bezpieczeństwa, ze wskazaniem, czy zdarzenie mogło zostać wywołane działaniem bezprawnym oraz czy mogło wywrzeć wpływ transgraniczny.
- Najpóźniej przed upływem 72 godzin od poważnego incyduentu firma musi przesłać raport zawierający wstępną ocenę jego skutków i dotkliwości, a w stosownych przypadkach – także wskaźników integralności systemów.
- Na wniosek właściwego Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT) lub innego organu właściwego organizacja musi złożyć sprawozdanie okresowe z aktualizacją statusu usuwania skutków incyduentu lub – nie później niż miesiąc od zgłoszenia incyduentu – sprawozdanie końcowe. Raport powinien zawierać szczegółowy opis zdarzenia, rodzaj zagrożenia lub pierwotną przyczynę jego wystąpienia, wszystkie podjęte środki zaradcze oraz analizę wszelkich skutków transgranicznych.
- Jeżeli incydent nie zakończył się w terminie składania raportu końcowego, organizacja przedstawia w tym terminie sprawozdanie z postępu prac, a sprawozdanie końcowe – w ciągu miesiąca od zakończenia obsługi zdarzenia.

5. Cel NIS2: zarządzanie ryzykiem

Centralnym elementem nowej dyrektywy NIS2 jest kompleksowe zarządzanie ryzykiem. Ogółem wymogi NIS2 przewidują, że działania w zakresie zarządzania ryzykiem muszą odpowiadać najnowszym mającym zastosowanie standardom, poziomowi narażenia na ryzyko, wielkości organizacji oraz prawdopodobieństwu wystąpienia incydentów bezpieczeństwa i ich dotkliwości. Działania te muszą również uwzględniać potencjalne skutki społeczne i ekonomiczne. Organizacje, które nie wdrażają środków zarządzania ryzykiem, robią to nieprawidłowo lub w nieodpowiednim czasie, naruszają przepisy NIS2.

W wielu firmach wdrożenie NIS2 wymaga początkowo podjęcia wielu czynności technicznych i organizacyjnych. NIS2 kładzie także nacisk na cyberhigienę i praktyki zapobiegania incydentom. Chociaż nie istnieje jedno narzędzie, które całkowicie spełniałoby wszystkie wymagania NIS2, większość firm już korzysta z licznych rozwiązań z zakresu bezpieczeństwa IT, które mogą pomóc im osiągnąć zgodność z dyrektywą. Obejmują one narzędzia do kontroli dostępu do sieci i monitorowania, [zarządzania klientami oraz zintegrowanego zarządzania punktami końcowymi](#) (UEM).

Zautomatyzowane narzędzia w systemie UEM mogą skutecznie pomóc firmom osiągnąć zgodność z szerokim zakresem wymagań NIS2, począwszy od kompleksowej [inwentaryzacji](#) sprzętu i oprogramowania. Ważne, by uwzględniać wszystkie typy urządzeń, w tym kontrolery i urządzenia sieciowe, jak również komputery i urządzenia mobilne. Zarządzanie zasobami sprzętowymi i [oprogramowaniem](#) jest podstawą do spełnienia niektórych wymagań NIS2, takich jak przejrzystość, analiza ryzyka i ogólne bezpieczeństwo informacji.

UEM oferuje również cenne narzędzia do automatycznej i niezawodnej obsługi technicznej oraz ochrony punktów końcowych, w tym zarządzanie [podatnościami](#) i aktualizacjami, szyfrowanie dysków, listy dozwolonego i blokowanego oprogramowania oraz system zgłoszeń do szybkiego rozwiązywania problemów.

Jakie środki zarządzania ryzykiem reguluje dyrektywa NIS2?

- **Polityki:** wprowadzenie wytycznych dotyczących zarządzania ryzykiem oraz wdrażania środków bezpieczeństwa informacji
- **Zarządzanie incydentami:** wykrywanie incydentów bezpieczeństwa i zarządzanie nimi
- **Ciągłość działania:** zarządzanie kopiami zapasowymi, odzyskiwanie danych po awarii oraz zarządzanie kryzysowe
- **Łańcuch dostaw:** środki zabezpieczające procesy zaopatrzenia, utrzymania i obsługi systemów IT i sieci
- **Skuteczność:** specyfikacje dla oceny cyberryzyka i wdrażania odpowiednich środków
- **Szkolenia:** regularne szkolenia z zakresu cyberbezpieczeństwa dla kadry kierowniczej i pracowników
- **Bezpieczeństwo danych:** wymogi dotyczące szyfrowania we wszystkich kluczowych obszarach
- **Personel:** ochrona danych osobowych pracowników
- **Kontrola dostępu:** monitorowanie i rejestrowanie aktywności w sieci
- **Zarządzanie zasobami:** zgodność zasad, procedur, metod i narzędzi systemów zarządzania bezpieczeństwem informacji (ISMS) z normą ISO 27001
- **Uwierzytelnianie:** stosowanie uwierzytelniania wieloskładnikowego (MFA) i pojedynczego logowania (SSO)
- **Komunikacja:** szyfrowanie komunikacji głosowej, wideo i tekstowej
- **Reagowanie kryzysowe:** stosowanie bezpiecznych systemów komunikacji awaryjnej

6.Z baramundi do zgodności z NIS2

Czy odpowiadasz za IT w firmie objętej dyrektywą NIS2? W takim razie baramundi może pomóc Ci w spełnieniu obowiązujących Twoje przedsiębiorstwo nowych wymagań dotyczących cyberbezpieczeństwa. Pakiet baramundi Management Suite obejmuje następujące obszary dyrektywy NIS2 wraz z wymienionymi poniżej funkcjami:

Artykuł 21 **Środki zarządzania ryzykiem w cyberbezpieczeństwie**

Państwa członkowskie zapewniają, aby podmioty [...] wprowadzały odpowiednie [...] środki [...] w celu zarządzania ryzykiem dla bezpieczeństwa sieci i systemów informatycznych [...] oraz w celu [...] minimalizowania wpływu incydentów.

a) Konceptcje związane z analizą ryzyka i bezpieczeństwem systemów informatycznych;

- **baramundi Vulnerability Scanner**
- **baramundi Inventory**
- **baramundi OT-Inventory**
- **baramundi Network Devices**
- **baramundi Update Management & Managed Software**

f) konceptcje i procedury z zakresu oceny skuteczności środków zarządzania ryzykiem w obszarze cyberbezpieczeństwa

- **baramundi Vulnerability Scanner**

h) konceptcje i procedury związane ze stosowaniem kryptografii, a także, w stosownych przypadkach, szyfrowania;

- **baramundi Endpoint Security**

i) Bezpieczeństwo personelu, konceptcje kontroli dostępu i zarządzanie aktywami

- **baramundi Endpoint Security**

Skuteczne rozwiązanie UEM, takie jak [baramundi Management Suite](#), nie tylko zapewnia ochronę przed karami, ale też zapobiega kosztownym przestojom. Zgodność z wytycznymi NIS2 jest zatem nie tylko obowiązkiem prawnym, ale także kluczowym wkładem w bezpieczeństwo i odporność całej firmy.

6. Kolejne kroki w kierunku zgodności z NIS2

Dla osób odpowiedzialnych za IT w organizacjach objętych przepisami NIS2 kluczowy jest czas. W miarę jak państwa UE wprowadzają lub aktualizują krajowe wymagania w zakresie zgodności z NIS2, konieczne jest szybkie i staranne planowanie, wdrożenie oraz regularna ocena środków z zakresu cyberbezpieczeństwa.

Zalecamy podjęcie następujących kroków:

1. **Zacznij od analizy skutków:** przeprowadź analizę wpływu, aby zaszerzować swoją firmę zgodnie z jej klasyfikacją działalności gospodarczej i dyrektywą NIS2. Zapewni to podstawę do planowania i wdrażania środków zgodności.
2. **Aktywnie zaangażuj zarząd w procesy związane z NIS2:** wyjaśnij zarządowi potencjalne skutki braku zgodności z dyrektywą lub opóźnienia w jej wdrażaniu, jednocześnie informując o korzyściach z proaktywnej implementacji. Opisz, jak NIS2 może długofalowo wzmocnić cyberodporność firmy i jej reputację.
3. **Zaplanuj środki zarządzania ryzykiem:** przeprowadź kompleksową analizę luk, aby określić, gdzie należy podjąć działania oraz jakie kroki są wymagane do poprawy cyberbezpieczeństwa. Zidentyfikuj odpowiednie rozwiązania do automatyzacji IT, które mogą uwolnić cenne zasoby zarówno do wdrażania niezbędnych środków, jak i bieżących zadań IT.
4. **Zdefiniuj i rozpocznij projekt wdrożenia NIS2:** zainicjuj dedykowany projekt wdrożeniowy, aby zapewnić terminowe osiągnięcie zgodności. Uwzględnij projekt w planach budżetowych i kadrowych.
5. **Zakończ rejestrację i przygotuj procesy raportowania:** ustanów procesy na potrzeby terminowej rejestracji i przygotuj procedury raportowania na wypadek poważnego incydentu bezpieczeństwa. Przetestuj i przećwicz te procesy, aby w nagłych wypadkach móc działać szybko i efektywnie.
6. **Utwórz system monitorowania regulacji:** ustanów system monitorowania, aby na bieżąco śledzić aktualne, planowane lub nowe przepisy. Dokładnie je analizuj i oceniaj ich wpływ na twoją firmę.
7. **Priorytetowo traktuj szkolenia:** Tylko w Niemczech trzy miliony managerów i pracowników będą musiały przechodzić szkolenia w ramach NIS2 każdego roku. Odpowiedni podmiot w każdym państwie członkowskim UE będzie na bieżąco dostarczać szczegółowe informacje na temat wymagań szkoleniowych.

Nie da się ukryć, że NIS2 wymaga rygorystycznego podejścia do cyberbezpieczeństwa oraz szybkiego i konsekwentnego wdrażania odpowiednich środków. Jest to kwestia, którą zarówno zarząd firmy, jak i działy IT muszą traktować poważnie, nie tylko ze względu na ryzyko sankcji administracyjnych, finansowych, a nawet karnych za naruszenia czy zaniedbania. W

istocie zgodność z NIS2 może wzmocnić ogólne cyberbezpieczeństwo i cyberodporność Twojej organizacji oraz symbolizować jej zaangażowanie w implementację solidnych mechanizmów bezpieczeństwa i działań zapobiegających szkodliwym cyberatakom. Skuteczne rozwiązanie UEM odgrywa kluczową rolę w pomaganiu zespołom IT w osiągnięciu i utrzymaniu zgodności, jednocześnie zmniejszając ryzyko jej braku. Ponadto UEM poprawia efektywność IT, jakość usług oraz wydajność i niezawodność systemu w codziennej działalności.

Chcesz dowiedzieć się więcej?

Więcej informacji o tym, jak wykorzystać automatyzację UEM do wsparcia zgodności z NIS2, jednocześnie poprawiając bezpieczeństwo i efektywność IT, uzyskasz odwiedzając naszą stronę internetową: <https://www.baramundi.com> lub kontaktując się z nami celem umówienia indywidualnej konsultacji.

Zapraszamy również do samodzielnego wypróbowania naszych rozwiązań UEM poprzez zapisy na bezpłatną, w pełni funkcjonalną, 30-dniową wersję próbną baramundi Management Suite na stronie <https://www.baramundi.com/management-suite/>.

Chcielibyśmy Cię poznać!

Skontaktuj się z nami!



baramundi software GmbH
Forschungsallee 3
86159 Augsburg, Germany

 +49 821 5 67 08 - 380
request@baramundi.com
www.baramundi.com

 +44 2071 93 28 77
request@baramundi.com
www.baramundi.com

 +48 735 91 44 54
request@baramundi.com
www.baramundi.com

 +49 821 5 67 08 - 390
request@baramundi.com
www.baramundi.com

 +43 19 28 01 36 00 10
request@baramundi.com
www.baramundi.com

 +39 340 8861886
request@baramundi.com
www.baramundi.com

 +41 77 280 49 79
request@baramundi.com
www.baramundi.com

baramundi software USA, Inc.
30 Speen St, Suite 501
Framingham, MA 01701, USA

 +1 508-861-7561
requestUSA@baramundi.com
www.baramundi.com