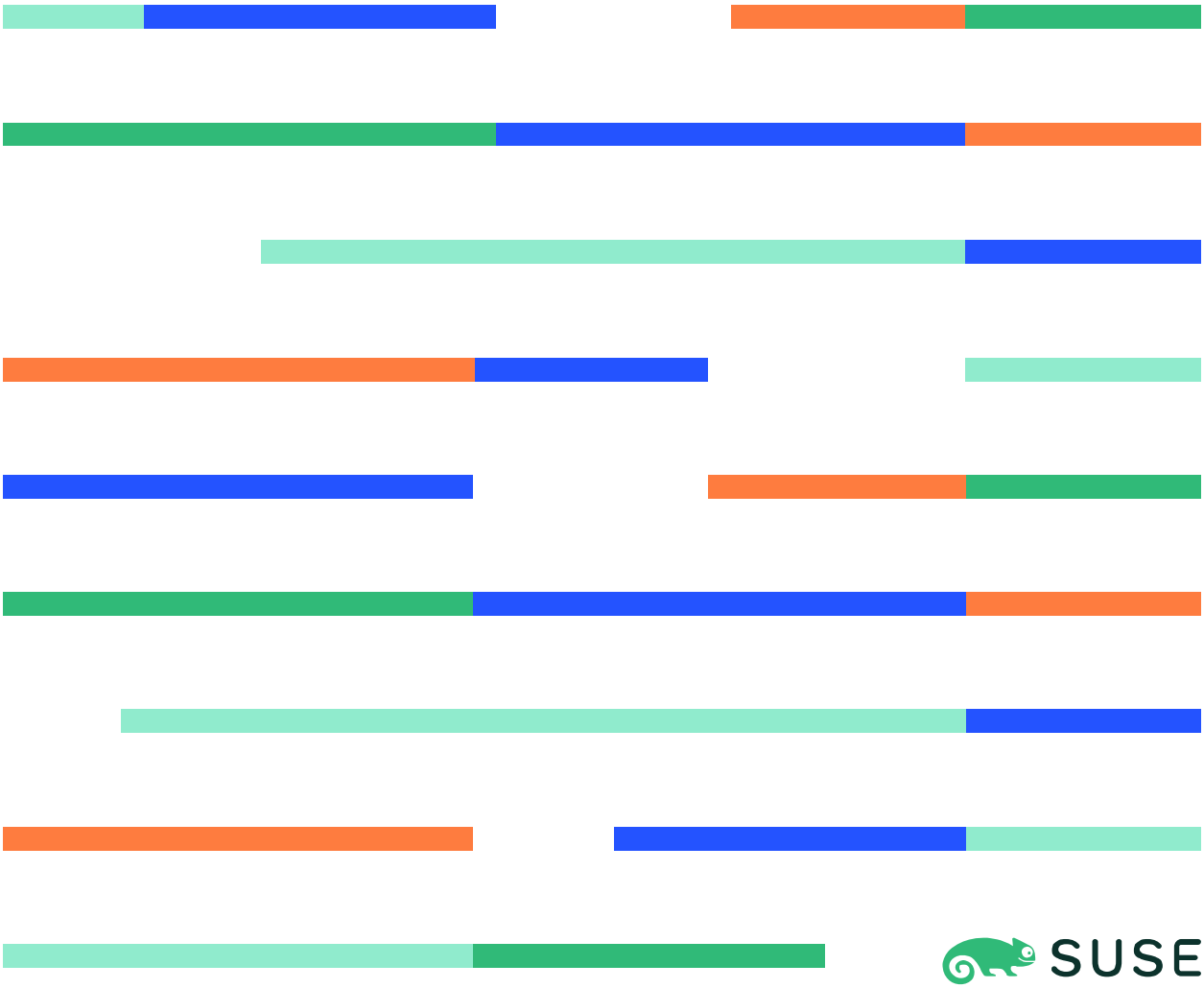
Zgodność z NIS-2

Sześć powodów, dla których warto już teraz wdrożyć oprogramowanie SUSE, aby zapewnić zgodność z nowymi wymogami w zakresie bezpieczeństwa sieci i informacji



SUSE

Zgodność z NIS-2: sześć powodów, dla których warto wdrożyć oprogramowanie SUSE

W nadchodzących miesiącach dziesiątki tysięcy firm i organizacji w Polsce będą musiały spełnić wymagania nowej dyrektywy UE w sprawie bezpieczeństwa sieci i informacji - w skrócie NIS-2. Przygotowywana w kraju ustawa implementuje wytyczne tej dyrektywy i powinna dostać uchwalona najpóźniej w październiku. SUSE pomaga w osiągnięciu pełnej zgodności z wytycznymi NIS-2 z odpowiednim wyprzedzeniem. Dzięki naszym rozwiązaniom można zwiększyć poziom bezpieczeństwa i niezawodności IT, zapewnić większą przejrzystość dbania o cyberbezpieczeństwo i szybciej osiągnąć wymagany poziom zgodności z przepisami.

Implementacja unijnej dyrektywy NIS-2 posuwa się szybko naprzód. W Polsce przygotowano projekt nowej ustawy dostosowującej do niej kwestie cyberbezpieczeństwa. W najbliższych miesiącach będzie ona procedowana w sejmie i powinna wejść w życie najpóźniej w październiku 2024. Przepisy NIS-2 mają bezpośredni wpływ na dziesiątki tysięcy firm i organizacji publicznych w Polsce, ponieważ obejmują bardzo wiele sektorów gospodarki. Ponadto ze względu na zależności w łańcuchach dostaw, ustawa będzie miała wpływ na jeszcze szerszy krąg organizacji i przedsiębiorstw.

Nawet jeśli nie jest jeszcze pewne czy nowe prawo wejdzie w życie 17 października 2024 r., jak to zaplanowano, kierownictwo przedsiębiorstw i menedżerowie IT powinni już teraz podjąć niezbędne działania technologiczne i organizacyjne. Wynika to z faktu, że NIS-2 nie tylko zwiększa wymagania dotyczące bezpieczeństwa sieci i informacji, ale także znacznie zwiększa zagrożenie karami za naruszenie przepisów. Członkowie zarządu są również osobiście odpowiedzialni za zapewnienie wdrożenia zalecanych środków. Przepisy te mają znacznie większy wpływ na funkcjonowanie firmy i potencjalne zakłócenia niż przepisy RODO (implementacja unijnych wytycznych GDPR).

Dlatego też zainteresowanym organizacjom i ich menedżerom zaleca się poważne potraktowanie wymogów dyrektywy NIS-2 oraz wdrożenie skutecznych strategii i rozwiązań w celu zabezpieczenia infrastruktury IT, aby uniknąć odpowiedzialności swoich członków zarządu. Projekt ustawy po raz kolejny wskazuje, że kwestie regulacji dotyczyć będą wszystkich systemów informatycznych organizacji sklasyfikowanych jako krytyczne – w tym na przykład serwerów, na których działa oprogramowanie księgowe, a to dotyczy przecież niemal każdej firmy.

Jak SUSE pomaga przygotować się do NIS-2

SUSE pomaga organizacjom i instytucjom rządowym spełnić wymagania NIS-2 na wiele sposobów. W szczególności potwierdzono, że nasze rozwiązania wzmacniają bezpieczeństwo infrastruktur IT w sześciu obszarach, ułatwiając zachowanie zgodności z nowymi przepisami.

1. Bezpieczeństwo łańcucha dostaw

NIS-2 wymaga od wszystkich zainteresowanych organizacji ciągłej oceny potencjalnych zagrożeń cybernetycznych w ich łańcuchu dostaw i podejmowania odpowiednich środków bezpieczeństwa. Jednak dla użytkowników oprogramowania przeprowadzenie niezależnej oceny całego łańcucha dostaw oprogramowania jest prawie niemożliwe. Wymagałoby to ogromnego nakładu czasu, a jednocześnie zawsze istniałoby ryzyko pociągnięcia do odpowiedzialności za przeoczoną lukę w zabezpieczeniach.

SUSE upraszcza ten proces dla wszystkich rozwiązań działających pod kontrolą systemu SUSE Linux Enterprise Server (SLES): System operacyjny posiada certyfikat Common Criteria EAL 4+ wydany przez niemiecki Federalny Urząd ds. Bezpieczeństwa Informacji (BSI). Oznacza to, że SUSE jest obecnie jedynym dostawcą systemu operacyjnego ogólnego przeznaczenia, który pomyślnie przeszedł kompleksową ocenę produktu, procesów rozwoju i aktualizacji zabezpieczeń. Ten oficjalnie uznany certyfikat zwalnia firmy z konieczności przeprowadzania własnej oceny i umożliwia im udowodnienie w dowolnym momencie, że bezpieczeństwo łańcucha dostaw ich systemu operacyjnego zostało przetestowane przez niezależny organ.

Rancher Prime - opracowana przez SUSE platforma do zarządzania kontenerami dla przedsiębiorstw - wspiera również zabezpieczanie łańcucha dostaw oprogramowania. Rozwiązanie uzyskało ostatnio certyfikat zgodności z Supply-chain Levels for Software Artifacts (SLSA). Ramy te, opracowane przez Google, mają na celu zapewnienie integralności oprogramowania podczas tworzenia plików binarnych. Środki takie jak zautomatyzowany proces kompilacji i pełna dokumentacja pochodzenia (Software Bill of Material = SBOM) chronią oprogramowanie przed manipulacją i umożliwiają bezpieczne śledzenie kodu źródłowego.

2. Szyfrowanie

Kolejnym ważnym aspektem NIS-2 jest kwestia kryptografii. Artykuł 21 dyrektywy wymaga, aby wszystkie zainteresowane organizacje korzystały z aktualnych technologii szyfrowania w celu zapewnienia bezpieczeństwa i integralności wrażliwych danych. SUSE pomaga organizacjom w implementacji i kieruje się opracowanymi przez rząd USA Federal Information Processing Standards (FIPS) 140-2 i 140-3, które definiują wymagania bezpieczeństwa, jakie muszą spełniać moduły kryptograficzne w amerykańskich agencjach rządowych.

SLES 15 SP2 posiada certyfikat FIPS 140-2, dzięki czemu zapewnia bezpieczną podstawę dla szyfrowanej komunikacji i przechowywania danych. Certyfikowane moduły kryptograficzne mogą być również używane w SP3. Moduły kryptograficzne SLES 15 SP4 przechodzą obecnie proces certyfikacji dla kolejnego standardu FIPS 140-3. Jak tylko audyt ze strony National Institute of Standards and Technology zostanie zakończony, odpowiednie moduły, takie jak Kernel Crypto API, GnuTLS, libgcrypt, mozilla-nss i OpenSSL zostaną certyfikowane zgodnie z tym standardem.

3. Rozwiązania wysokiej dostępności

Aby zachować zgodność z wymogami NIS-2 i DORA (Digital Operational Resilience Act), wiele organizacji musi zwiększyć odporność swojej infrastruktury informatycznej i podjąć dodatkowe działania w celu zapewnienia ciągłości działania. SUSE oferuje rozwiązania, które zapewniają maksymalną dostępność systemów i minimalizują przestoje. Obejmują one na przykład rozszerzenie SUSE Linux Enterprise High Availability Extension. Dzięki takim funkcjom, jak tworzenie klastrów geograficznych, replikacja danych między lokalizacjami i przełączanie awaryjne oparte na regułach, organizacje mają pewność, że ich najważniejsze aplikacje IT są zawsze dostępne, a działalność biznesowa może zostać szybko wznowiona nawet po nieprzewidzianych zdarzeniach.

4. Edge computing i bezpieczeństwo IoT

NIS-2 dotyczy wszystkich operatorów infrastruktury krytycznej w sektorach takich jak dostawy energii, produkcja, telekomunikacja, transport i logistyka. Obecnie organizacje te często wykorzystują urządzenia brzegowe i IoT do kontrolowania infrastruktury krytycznej. Urządzenia te i aplikacje dostarczane w środowiskach brzegowych muszą być również chronione przed potencjalnymi zagrożeniami cybernetycznymi.

SUSE Edge 3.0 może tu znacząco pomóc. Stos technologiczny oparty na Rancher, NeuVector i SLE Micro nie tylko upraszcza zarządzanie rozproszonymi urządzeniami, ale także oferuje kompleksowe funkcje bezpieczeństwa dla infrastruktur brzegowych każdej wielkości. Dzięki NeuVector, na przykład, polityki bezpieczeństwa mogą być egzekwowane we wszystkich obszarach, a ataki na środowiska brzegowe mogą być odpierane w czasie rzeczywistym. SLE Micro zwiększa bezpieczeństwo urządzeń brzegowych dzięki preinstalowanej strukturze bezpieczeństwa SELinux i niezmiennemu systemowi plików. Ponadto system operacyjny oferuje możliwość włączenia trybu FIPS w celu zapewnienia ścisłej zgodności z modułami kryptograficznymi zatwierdzonymi przez NIST i zastosowania najlepszych praktyk w zakresie wzmacniania systemu.

5. Zarządzanie podatnościami i ryzykiem dla kontenerów i Kubernetes

Wiele organizacji modernizuje obecnie swoje środowisko aplikacji i w coraz większym stopniu polega na aplikacjach natywnych dla chmury, które są opracowywane w sposób elastyczny i wdrażane w bardzo dynamiczny sposób. Ten aspekt również należy wziąć pod uwagę przy planowaniu realizacji strategii NIS-2. SUSE NeuVector oferuje kompleksowe zarządzanie lukami w zabezpieczeniach, zautomatyzowane zabezpieczenia potoku CI/CD, kompletne zabezpieczenia środowiska uruchomieniowego oraz ochronę przed

zagrożeniami typu zero-day i zagrożeniami wewnętrznymi w środowisku Kubernetes. Jednocześnie rozwiązanie do zabezpieczania kontenerów sprawdza i kontroluje dostęp podczas opracowywania, testowania i wdrażania nowych aplikacji. SUSE NeuVector skanuje kontenery, hosty i platformy orkiestracji w czasie ich działania oraz weryfikuje bezpieczeństwo hostów i kontenerów. Wszystkie te funkcje pomagają organizacjom zachować zgodność z wytycznymi NIS-2 dotyczącymi obciążeń skonteneryzowanych.

6. Ulepszone raportowanie incydentów

Dyrektywa NIS-2 obejmuje również rozszerzone obowiązki sprawozdawcze w przypadku zaistnienia incydentów bezpieczeństwa. Dotknięte organizacje muszą poinformować odpowiedzialne organy rządowe o incydencie w ciągu 24 godzin. Najpóźniej po 72 godzinach są one zobowiązane do złożenia kompleksowego raportu. Wymóg ten jest również łatwiejszy do spełnienia dzięki SUSE: produkty takie jak SUSE Manager, Rancher i NeuVector mają wszechstronne możliwości monitorowania i raportowania. Narzędzia te pomagają monitorować stan infrastruktury IT w czasie rzeczywistym, wykrywać anomalie i szybko identyfikować incydenty bezpieczeństwa oraz automatyzować związane z nimi procesy. Pomagają również w gromadzeniu informacji wymaganych do zbadania incydentu i zgłoszenia go odpowiednim organom.

Zapraszamy do rozmów

Zespół SUSE Polska jest do Państwa dyspozycji. Zapraszamy do kontaktu z nami i rozmów o wsparciu Państwa organizacji w spełnieniu już teraz wymogów dyrektywy NIS-2.

SUSE Polska Sp. z o.o.
ul. Postępu 21
02-676 Warszawa

tel. +48 22 537 5020
e-mail: infolinia@suse.com

www.suse.pl