ZABBIX

Zabbix + NIS2 =
spokój audytora

ZABBIX

O mnie

- Administrator Linux / SysOps
- Z pasją do monitoringu i automatyzacji
- Zabbix Certified Expert (+ZCS i ZCP)

Michał Kudłacz | Technical Support Engineer @ Zabbix

NIS vs NIS2

ZABBIX

NIS (2016/1148) – pierwsza dyrektywa UE o cyberbezpieczeństwie (2016), obejmowała m.in. operatorów usług kluczowych i wybranych dostawców usług cyfrowych.

NIS2 (2022/2555) – nowa dyrektywa:

- wejście w życie: styczeń 2023 (20 dni po publikacji)
- transpozycja do prawa krajowego: **do 17.10.2024**
- stosowanie przepisów krajowych: **od 18.10.2024**
- rozszerzony zakres: podmioty **kluczowe** i **ważne** w sektorach z załączników I–II (energia, zdrowie, transport, infrastruktura cyfrowa, administracja itd.)

Sektory podlegające pod NIS2

ZABBIX

Energetyka

Podmiot kluczowy

Opieka zdrowotna

Podmiot kluczowy

Transport

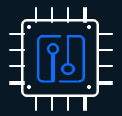
Podmiot kluczowy

Bankowość

Podmiot kluczowy

Woda pitna / ścieki

Podmiot kluczowy



Infrastruktura cyfrowa

Podmiot kluczowy

Administracja publiczna

Podmiot kluczowy

Dostawcy cyfrowi

Podmiot ważny

Usługi kurierskie

Podmiot ważny

Gospodarka odpadami

Podmiot ważny

Przestrzeń kosmiczna

Podmiot kluczowy

Żywność

Podmiot ważny

Produkcja

Podmiot ważny

Produkcja chemikaliów

Podmiot ważny

Badania naukowe

Podmiot ważny

Sektory podlegające pod NIS2 c.d.

ZABBIX

Zarządzanie usługami ICT (MSP/MSSP) - podmiot kluczowy

Bankowość i infrastruktura rynków finansowych - podmiot kluczowy

Infrastruktura cyfrowa (DNS, TLD, usługi chmurowe, CDN) – podmiot kluczowy

Dostawcy internetowych platform handlowych, wyszukiwarek internetowych i platform usług sieci społecznościowych (dostawcy cyfrowi) - podmiot ważny

NIS2 - kary administracyjne

Podmioty kluczowe:
do 10 mln EUR albo 2% globalnego rocznego obrotu

Podmioty ważne:
do 7 mln EUR albo 1,4% globalnego rocznego obrotu

W obu przypadkach stosuje się wyższą z kwot

Zgodność z NIS2: jak Zabbix może pomóc

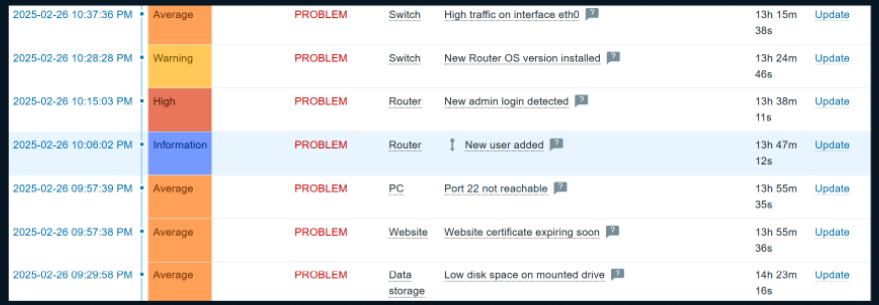
- Analiza ryzyka i bezpieczeństwo
- Reagowanie na incydenty
- Backup i recovery
- Bezpieczeństwo łańcucha dostaw
- Bezpieczeństwo systemów i podatności
- Kryptografia i szyfrowanie
- Bezpieczeństwo HR i kontrola dostępu
- Uwierzytelnianie wieloskładnikowe (MFA)

Analiza ryzyka i bezpieczeństwo systemów informatycznych

ZABBIX

Zabbix może:

- wykryć anomalie, przeciążenie zasobów, brak dostępności itd.
- monitorować obciążenie sieci, zbierać metryki interfejsów sieciowych I innych usług krytycznych
- sprawdzać otwartość portów, monitorować certyfikaty SSL
- monitorować integralność ważnych plików np. konfiguracyjnych
- utworzyć własny workflow i powiadomienia
- monitorować czujniki w centrach danych aby wykryć włamania



2025-02-26 10:37:36 PM	Average	PROBLEM	Switch	High traffic on interface eth0	13h 15m 38s	Update
2025-02-26 10:28:28 PM	Warning	PROBLEM	Switch	New Router OS version installed	13h 24m 46s	Update
2025-02-26 10:15:03 PM	High	PROBLEM	Router	New admin login detected	13h 38m 11s	Update
2025-02-26 10:06:02 PM	Information	PROBLEM	Router	New user added	13h 47m 12s	Update
2025-02-26 09:57:39 PM	Average	PROBLEM	PC	Port 22 not reachable	13h 55m 35s	Update
2025-02-26 09:57:38 PM	Average	PROBLEM	Website	Website certificate expiring soon	13h 55m 36s	Update
2025-02-26 09:29:58 PM	Average	PROBLEM	Data storage	Low disk space on mounted drive	14h 23m 16s	Update

NIS2 REQUIREMENT 1

Reagowanie na incydenty bezpieczeństwa

ZABBIX

Dyrektywa NIS2 nakłada obowiązek wdrożenia skutecznych procedur obsługi incydentów bezpieczeństwa, w tym ich wykrywania, eskalacji, analizy, raportowania oraz zarządzania.

- System alertów i eskalacji
- Przyspieszona reakcja na incydenty
- Wielokanałowe powiadomienia w czasie rzeczywistym
- Wysyłanie wiadomości przez e-mail, SMS, Webhooki
- Automatyczne rozwiązywanie problemów poprzez wykonywanie skryptów lub komend na agencie lub serwerze
- Eskalacja problemów zgodnie z elastycznymi poziomami usług (SLA) definiowanymi przez użytkownika
- Personalizowanie powiadomień w zależności od roli odbiorcy (np. administrator IT otrzyma pełny raport o awarii, a dyrektor operacyjny tylko podsumowanie wpływu na biznes)

Backup & Disaster Recovery

ZABBIX

Monitorowanie procesu kopii zapasowych

Zabbix umożliwia:

- monitorowanie platform backupowych (Veeam, Bacula i inne)
- nadzór nad procesem wykonywania kopii zapasowych
- śledzenie pojemności i wykorzystania serwerów backupowych

Name ▲	Triggers	Key	Interval	History	Trends	Type	Status	Tags
Get metrics: Failed Job Runs	Triggers 1	veeam.manager.failed.jobs		Stored	Stored	Dependent item	Enabled	component: reports
Get metrics: Get errors	Triggers 1	veeam.manager.get.errors		Stored		Dependent item	Enabled	component: status
Get metrics		veeam.manager.get.metrics	5m	Not stored		Script	Enabled	component: raw
Get metrics: Running Jobs		veeam.manager.running.jobs		Stored	Stored	Dependent item	Enabled	component: reports
Get metrics: Scheduled Backup Jobs		veeam.manager.scheduled.backup.jobs		Stored	Stored	Dependent item	Enabled	component: reports
Get metrics: Scheduled Jobs		veeam.manager.scheduled.jobs		Stored	Stored	Dependent item	Enabled	component: reports
Get metrics: Scheduled Replica Jobs		veeam.manager.scheduled.replica.jobs		Stored	Stored	Dependent item	Enabled	component: reports
Get metrics: Total Job Runs		veeam.manager.scheduled.total.jobs		Stored	Stored	Dependent item	Enabled	component: reports

Bezpieczeństwo łańcucha dostaw

ZABBIX

Monitorowanie systemów dostawców, w tym relacje pomiędzy każdą jednostką orez dostępność i jakość usług zewnętrznych i zależności

Użytkownicy mogą konfigurować progi ostrzegawcze i automatyczne powiadomienia o przekroczeniach ustalonych wskaźników (KPI)

Name	Status	Root cause
Backend application	OK	
Backup environment	High	Backup node 5 down
MySQL database	OK	
Web application	Average	High session count, Web application node 1 down, High request count
Zabbix application server	OK	

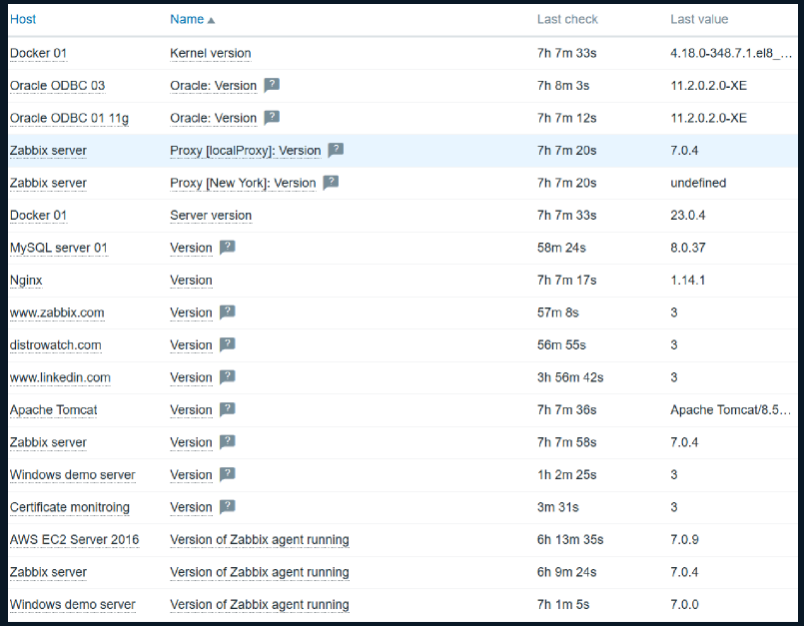
NIS2 REQUIREMENT 4

Bezpieczeństwo systemów i podatności

ZABBIX

Zabbix umożliwia monitorowanie zmian w środowisku IT, takich jak nowe instalacje, aktualizacje komponentów czy nieautoryzowane zmiany w konfiguracji.

- śledzenie wersji oprogramowania
- monitorowanie zmian
- identyfikacja przestarzałych komponentów
- Integracja z zewnętrznymi narzędziami w celu sprawdzania podatności



Host	Name ▲	Last check	Last value
Docker 01	Kernel version	7h 7m 33s	4.18.0-348.7.1.el8_...
Oracle ODBC 03	Oracle: Version	7h 8m 3s	11.2.0.2.0-XE
Oracle ODBC 01 11g	Oracle: Version	7h 7m 12s	11.2.0.2.0-XE
Zabbix server	Proxy [localProxy]: Version	7h 7m 20s	7.0.4
Zabbix server	Proxy [New York]: Version	7h 7m 20s	undefined
Docker 01	Server version	7h 7m 33s	23.0.4
MySQL server 01	Version	58m 24s	8.0.37
Nginx	Version	7h 7m 17s	1.14.1
www.zabbix.com	Version	57m 8s	3
distrowatch.com	Version	56m 55s	3
www.linkedin.com	Version	3h 56m 42s	3
Apache Tomcat	Version	7h 7m 36s	Apache Tomcat/8.5...
Zabbix server	Version	7h 7m 58s	7.0.4
Windows demo server	Version	1h 2m 25s	3
Certificate monitroing	Version	3m 31s	3
AWS EC2 Server 2016	Version of Zabbix agent running	6h 13m 35s	7.0.9
Zabbix server	Version of Zabbix agent running	6h 9m 24s	7.0.4
Windows demo server	Version of Zabbix agent running	7h 1m 5s	7.0.0

Kryptografia i szyfrowanie

ZABBIX

Dyrektywa NIS2 nakłada na organizacje obowiązek stosowania odpowiednich technik kryptograficznych, w kryptograficznych, w tym monitorowania używanych certyfikatów i szyfrowania danych.

Monitoring certyfikatów i mechanizmów szyfrowania

Powiadomienia o wygasających certach

Szyfrowanie pomiędzy komponentami

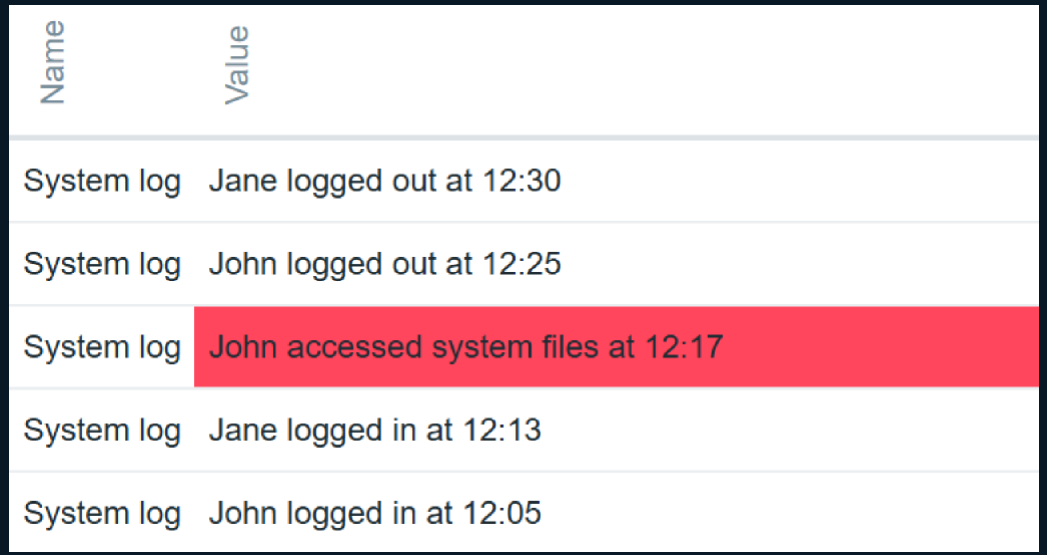
PSK, TLS, vault

Host	Name ▲	Last check	Last value
www.zabbix.com	Expires on	55m 52s	2025-04-22 04:41:...
www.zabbix.com	Fingerprint	55m 52s	409fe48b8fae079c...
www.zabbix.com	Get		
www.zabbix.com	Issuer	55m 52s	CN=WE1,O=Googl...
www.zabbix.com	Last validation status	55m 52s	certificate verified s...
www.zabbix.com	Public key algorithm	55m 52s	ECDSA
www.zabbix.com	Serial number	55m 52s	f7297e54ed7b769f...
www.zabbix.com	Signature algorithm	55m 52s	ECDSA-SHA256
www.zabbix.com	Subject	55m 52s	CN=zabbix.com
www.zabbix.com	Subject alternative name	55m 52s	["zabbix.com","*.za...
www.zabbix.com	Validation result	55m 52s	valid
www.zabbix.com	Valid from	55m 52s	2025-01-22 02:41:...
www.zabbix.com	Version	55m 52s	3

HR i kontrola dostępu

ZABBIX

Dyrektywa NIS2 nakłada na organizacje obowiązek zapewnienia bezpieczeństwa dostępu do systemów i danych poprzez odpowiednie zarządzanie użytkownikami oraz kontrolę ich aktywności. Kluczowe jest nie tylko ograniczenie dostępu do informacji wyłącznie do uprawnionych osób, ale także rejestrowanie działań użytkowników w celach audytowych i bezpieczeństwa.



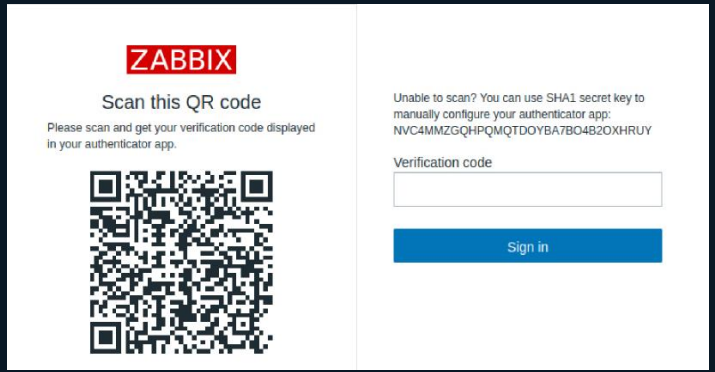
Name	Value
System log	Jane logged out at 12:30
System log	John logged out at 12:25
System log	John accessed system files at 12:17
System log	Jane logged in at 12:13
System log	John logged in at 12:05

Uwierzytelnienie wieloskładnikowe

Dyrektywa NIS2 wymaga od organizacji stosowania silnych mechanizmów uwierzytelniania, w tym rozwiązań wieloskładnikowych (MFA), oraz zapewnienia bezpieczeństwa komunikacji wewnętrznej i awaryjnej.

Zabbix umożliwia:

- monitoring wydajności i dostępności dostawców tożsamości (IdP)
- wykorzystanie API do pobierania informacji o politykach MFAi logowaniach
- analizę logów związanych z MFA
- tworzenie dashboardów i raportów dot. MFA



ZABBIX

Dyrektywa w języku polskim:

Dziękuję!