Zabezpieczenia dla IT

Zabezpieczenia z Załącznika A, które dotykają administratora, z dowodami do pokazania audytorowi.

- Zabezpieczenia dla IT po ludzku: dostęp, tożsamość i konta uprzywilejowane
- Zabezpieczenia dla IT po ludzku: systemy, sieć i dane
- Zabezpieczenia dla IT po ludzku: zmiany, dostawcy, incydenty i ciągłość działania

Zabezpieczenia dla IT po ludzku: dostęp, tożsamość i konta uprzywilejowane

Poziom: średnio

Dotyczy: ISO/IEC 27001:2022 Załącznik A: 5.3, 5.15 do 5.18, 6.5, 8.2 do 8.5, 8.18; Active Directory ad.zielona.example, Entra ID, Vaultwarden, Gitea, FreeIPA

Czas: ~40 min

Pierwsza z trzech stron o zabezpieczeniach, które dotykają pracy administratora. Dla każdego zabezpieczenia mówi, o co w nim naprawdę chodzi, co audytor chce zobaczyć i gdzie w tej bazie jest opis, jak to zrobiliśmy. Fiszka zbiera polecenia, które dają dowód: eksporty, listy i raporty, które kładziemy na stół w dniu audytu.

Numery i nazwy zabezpieczeń podajemy własnymi słowami, a ich sens parafrazujemy na podstawie publicznych opracowań ISO/IEC 27001:2022 i 27002:2022 [1][2]. „Co audytor chce zobaczyć” to nasze doświadczenie z publicznych list kontrolnych i rozmów, a nie lista z normy: jednostki mogą pytać inaczej.

Skróty użyte na tej stronie (11)

Skrót	Co znaczy
AD	Active Directory: katalog Microsoftu z kontami użytkowników, komputerów i grup w firmie
ASR	Attack Surface Reduction: reguły redukcji powierzchni ataku w Defenderze, które blokują zachowania typowe dla złośliwego oprogramowania, na przykład uruchamianie plików z makr Office albo kradzież haseł z pamięci systemu; w Azure także Azure Site Recovery: replikacja maszyn do innego regionu i przełączenie po awarii
GLPI	Gestionnaire Libre de Parc Informatique: otwarty system do zgłoszeń, inwentarza i bazy wiedzy IT; w Zielonej działa w kontenerze na docker01
gMSA	group Managed Service Account: konto usługi, któremu Windows sam zmienia hasło
ISMS	Information Security Management System: system zarządzania bezpieczeństwem informacji, czyli polityka, role, ocena ryzyka, cele, pomiar, audyt i doskonalenie, które decydują o zabezpieczeniach i sprawdzają, czy działają

Skrót	Co znaczy
ISO	International Organization for Standardization: organizacja, która wydaje normy techniczne używane na całym świecie
IT	Information Technology: dział albo praca związana z komputerami i infrastrukturą firmy
LAPS	Local Administrator Password Solution: mechanizm Windowsa nadający każdemu komputerowi inne, losowe hasło konta lokalnego administratora i zapisujący je w katalogu
MFA	Multi-Factor Authentication: logowanie drugim składnikiem, np. kodem z telefonu
VPN	Virtual Private Network: szyfrowany tunel do sieci firmowej
WMS	Warehouse Management System: system zarządzania magazynem

Fiszka

Polecenia PowerShell wykonujemy kontem `.admin` albo zwykłym kontem domenowym z prawem odczytu katalogu, na osobnej stacji administracyjnej. Żadne z nich nie zmienia systemu: tworzą tylko pliki z dowodami w katalogu `C:\IT\Audyt`.

□□ TYLKO ODCZYT

Eksport członków grup uprzywilejowanych do pliku dowodu: Get-ADGroupMember -Recursive

```
"Domain Admins","Enterprise Admins","Schema Admins","Administrators","Account Operators","Backup Operators","Server Operators","DnsAdmins" | ForEach-Object { $g = $_; Get-ADGroupMember -Identity $g -Recursive | Select-Object @{n='Grupa';e={$g}}, SamAccountName, objectClass } | Export-Csv "C:\IT\Audyt\uprzywilejowani-$(Get-Date -Format yyyy-MM-dd).csv" -NoTypeInformation -Encoding UTF8
```

Dowód do 8.2. Plik z datą w nazwie dołączamy co miesiąc do zadania w GLPI „Przegląd kont uprzywilejowanych”, razem z listą zatwierdzoną. Sama lista bez porównania nie jest dowodem kontroli, tylko zdjęciem.

Przykład:

```
"Grupa","SamAccountName","objectClass"
"Domain Admins","Administrator","user"
"Enterprise Admins","Administrator","user"
"DnsAdmins","jan.kowalski.t0","user"
```

GLPI = Gestionnaire Libre de Parc Informatique: otwarty system do zgłoszeń, inwentarza i bazy wiedzy IT; w Zielonej działa w kontenerze na docker01 · **IT** = Information Technology: dział albo praca związana z komputerami i infrastrukturą firmy

TYLKO ODCZYT

Sprawdzenie członkostw czasowych: Get-ADGroup -ShowMemberTimeToLive

```
Get-ADGroup -Identity "Domain Admins" -Properties member -ShowMemberTimeToLive | Select-Object -ExpandProperty member
```

Pokazuje członków z pozostałym czasem członkostwa w sekundach (zapis `<TTL=...>` przed nazwą). Dowód, że uprawnienia administratora domeny dajemy na godziny, a nie na zawsze, tak jak opisuje strona o hartowaniu AD.

Przykład:

```
<TTL=10412>,CN=jan.kowalski.t0,OU=Uzytkownicy,DC=ad,DC=zielona,DC=example
CN=Administrator,CN=Users,DC=ad,DC=zielona,DC=example
```

TTL = Time To Live: czas życia rekordu lub danych · **AD** = Active Directory: katalog Microsoftu z kontami użytkowników, komputerów i grup w firmie

TYLKO ODCZYT

Wyszukanie kont włączonych, nieużywanych od 90 dni: Search-ADAccount -AccountInactive

```
Search-ADAccount -AccountInactive -TimeSpan 90.00:00:00 -UsersOnly | Where-Object Enabled | Select-Object SamAccountName, LastLogonDate, DistinguishedName
```

Dowód do 5.16 i 5.18. Każde konto z tej listy wymaga decyzji: wyłączenie, wyjaśnienie (urlop macierzyński, konto techniczne) albo wpis wyjątku w GLPI. `LastLogonDate` replikuje się z opóźnieniem do 14 dni, więc próg 90 dni jest bezpieczny.

Przykład:

```
SamAccountName LastLogonDate        DistinguishedName
-------------- -------------        -----------------
jan.nowak      30.06.2026 15:42:10
```

```
CN=jan.nowak,OU=Biuro,OU=Uzytkownicy,DC=ad,DC=zielona,DC=example
skaner.test    02.03.2026 06:01:44
CN=skaner.test,OU=Magazyn,OU=Uzytkownicy,DC=ad,DC=zielona,DC=example
```

GLPI = Gestionnaire Libre de Parc Informatique: otwarty system do zgłoszeń, inwentarza i bazy wiedzy IT; w Zielonej działa w kontenerze na docker01

TYLKO ODCZYT

Wyeksportowanie włączonych kont do porównania z listą kadr: Get-ADUser -Filter Enabled

```
Get-ADUser -Filter 'Enabled -eq $true' -SearchBase
"OU=Uzytkownicy,DC=ad,DC=zielona,DC=example" -Properties Department, Title, whenCreated,
LastLogonDate | Select-Object SamAccountName, Name, Department, Title, whenCreated,
LastLogonDate | Export-Csv "C:\IT\Audyt\konta-wlaczone-$(Get-Date -Format yyyy-MM-
dd).csv" -NoTypeInformation -Encoding UTF8
```

Raz w miesiącu porównujemy ten plik z listą zatrudnionych, którą przysyła kadry. Każde włączone konto spoza listy to sprawa do wyjaśnienia tego samego dnia, a wynik porównania to zapis do 5.18 i 6.5.

OU = Organizational Unit: folder w Active Directory grupujący konta i komputery · **DC** = Domain Controller: serwer, który trzyma Active Directory i loguje użytkowników · **IT** = Information Technology: dział albo praca związana z komputerami i infrastrukturą firmy

TYLKO ODCZYT

Odczyt polityki haseł domeny: Get-ADDefaultDomainPasswordPolicy

```
Get-ADDefaultDomainPasswordPolicy -Identity NazwaDomeny | Select-Object
MinPasswordLength, ComplexityEnabled, MaxPasswordAge, LockoutThreshold, LockoutDuration
```

Dowód do 5.17 i 8.5. Wynik porównujemy z tym, co napisaliśmy w polityce i na stronie o zasadach haseł; rozjazd między dokumentem a domeną to gotowa niezgodność.

Przykład:

```
MinPasswordLength : 14
ComplexityEnabled : True
MaxPasswordAge    : 00:00:00
```

```
LockoutThreshold  : 10
LockoutDuration   : 00:15:00
```

□□ TYLKO ODCZYT

Sprawdzenie członków grupy administratorów na Linuksie: getent group

```
getent group wheel
```

Pokazuje lokalnych członków grupy `wheel`, czyli osoby z prawem `sudo` na serwerach Rocky Linux. Na serwerach w domenie FreeIPA sprawdzamy dodatkowo reguły sudo w FreeIPA. Lista ma być krótka i taka sama na każdym serwerze.

Przykład:

```
wheel:x:10:ansible
```

□□ **getent** = get entries: odpytaj bazę systemową (użytkowników, grup, hostów) niezależnie od tego, czy to plik lokalny czy AD

□□ KLIKAMY W INTERFEJSIE

Sprawdzenie rejestracji MFA w Entra ID: User registration details

```
entra.microsoft.com → Entra ID → Authentication methods → User registration details →
filtr: Multifactor authentication capable = No
```

Dowód do 8.5 dla kont chmurowych. Lista osób bez zarejestrowanej metody drugiego składnika trafia do kierowników działów z terminem. Nazwy menu sprawdzamy w portalu, bo Microsoft je zmienia.

□□ ZRZUT EKRANU DO UZUPEŁNIENIA

Zrzut do uzupełnienia: ekran User registration details w Entra ID z filtrem „Multifactor authentication capable = No”, widoczna liczba kont i kolumny Default method, Methods registered.

□□ **MFA** = Multi-Factor Authentication: logowanie drugim składnikiem, np. kodem z telefonu

KLIKAMY W INTERFEJSIE

Przegląd kont w Vaultwardenie: panel administracyjny, Users

```
hasla.zielona.example/admin → Users → kolumny: e-mail, 2FA, ostatnia aktywność,
organizacje
```

Dowód do 5.17 i 6.5: czy każde konto należy do obecnego pracownika i czy ma włączone logowanie dwuetapowe. Panel administracyjny otwieramy tylko z sieci VPN administratorów.

VPN = Virtual Private Network: szyfrowany tunel do sieci firmowej

TYLKO ODCZYT

Przegląd dostępu do kodu w Gitea: zespoły organizacji

```
git.zielona.example → Organizacja → Teams → każdy zespół: Members i Repositories →
uprawnienia Read, Write, Admin
```

Dowód do 8.4. Raz na kwartał Ola potwierdza listę osób z prawem zapisu do repozytoriów aplikacji, a my do repozytoriów konfiguracji. Potwierdzenie to komentarz w zadaniu GLPI z datą.

GLPI = Gestionnaire Libre de Parc Informatique: otwarty system do zgłoszeń, inwentarza i bazy wiedzy IT; w Zielonej działa w kontenerze na docker01

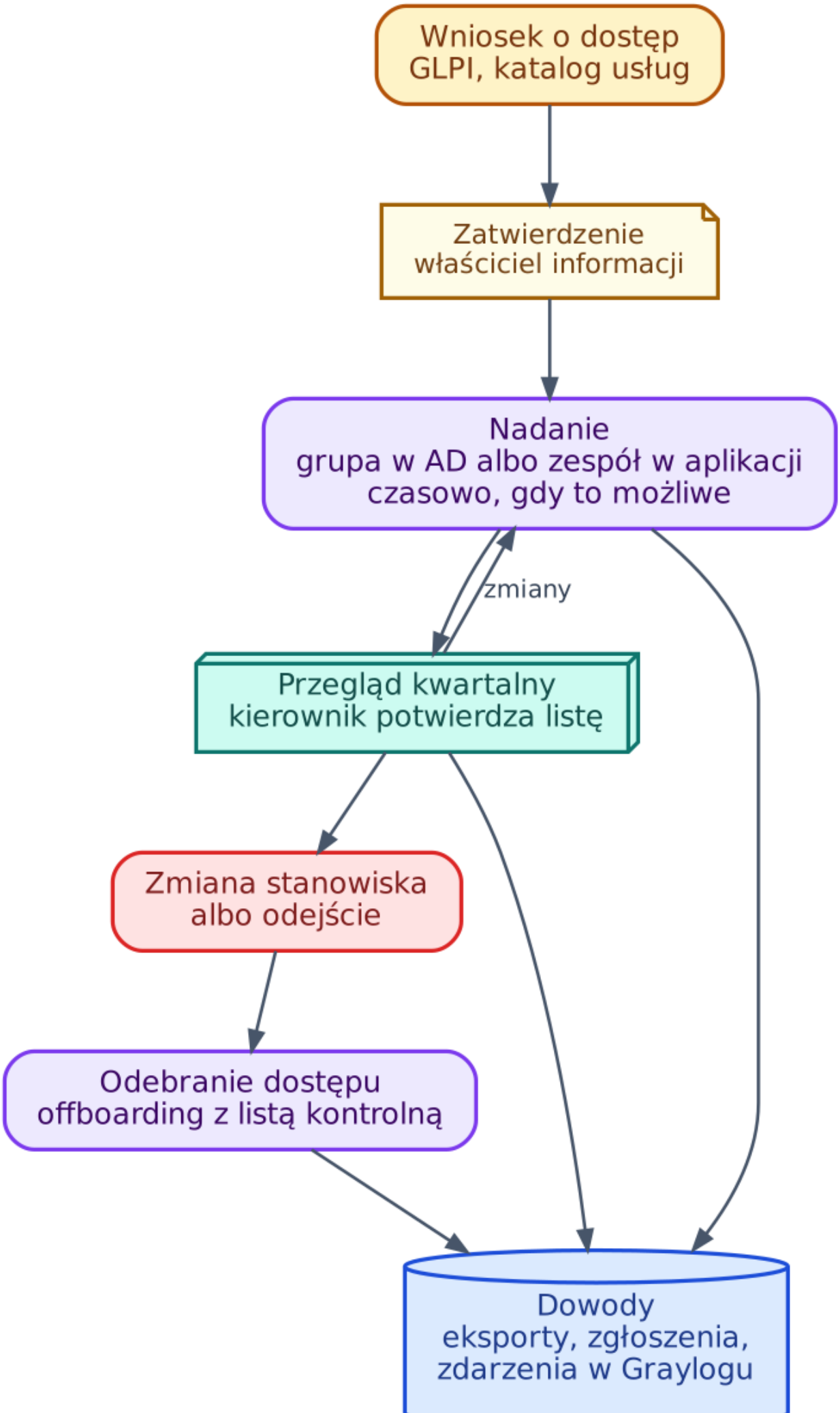
Z życia wzięte

Z ŻYCIA WZIĘTE

Poniedziałek, 19 października 2026, 9:00. Pan Wojtek przynosi listę 178 zatrudnionych od pani z kadr i prosi o listę włączonych kont w domenie. Plik z Fiszki ma 183 wiersze: dwa konta techniczne, które powinny być w osobnej jednostce, `skaner.test` z marca i `jan.nowak` z biura, który odszedł 30 czerwca, a jego konto VPN nadal działało. Tomek wyłącza konto przy panu Wojtku, ale ten prosi jeszcze o jedno: dowód, że od lipca nikt się na nie nie logował, i zapis, dlaczego offboarding w czerwcu się nie odbył.

Jak to działa

Wszystkie zabezpieczenia z tej strony opisują jeden cykl: konto powstaje na wniosek, dostaje tyle uprawnień, ile trzeba, jest przeglądane i znika, gdy przestaje być potrzebne. Audytor sprawdza, czy cykl jest zapisany, czy działa w praktyce i czy zostawia ślady.


Wniosek o dostęp
GLPI, katalog usług
Zatwierdzenie
właściciel informacji
Nadanie
grupa w AD albo zespół w aplikacji
czasowo, gdy to możliwe
zmiany
Przegląd kwartalny
kierownik potwierdza listę
Zmiana stanowiska
albo odejście
Odebranie dostępu
offboarding z listą kontrolną
Dowody
eksporty, zgłoszenia,
zdarzenia w Graylogu

Rysunek 1. Cykl życia dostępu w Zielonej: wniosek w GLPI, zatwierdzenie przez właściciela informacji, nadanie przez grupę w AD albo zespół w aplikacji, przegląd kwartalny przez kierownika, zmiana stanowiska albo odejście, odebranie dostępu i dowody: eksporty, zgłoszenia i zdarzenia w Graylogu (kliknięcie otwiera pełny rozmiar)

> **Pojęcie: zasada najmniejszych uprawnień.** Każda osoba i każdy program dostaje tylko te prawa, które są potrzebne do jego pracy, i tylko na czas tej pracy. To nie jest wyraz nieufności, tylko ograniczenie szkody: przejęte konto księgowej nie powinno otwierać repozytoriów Oli.

Zabezpieczenia po kolei

5.15 Kontrola dostępu: zapisane zasady, kto do czego

O co tu naprawdę chodzi. Firma ma zapisane zasady dostępu do informacji i systemów, oparte na potrzebach pracy i na bezpieczeństwie, i stosuje je tak samo w każdym systemie [1]. Nie chodzi o dokument, tylko o to, żeby na pytanie „dlaczego Kasia ma dostęp do udziału księgowości” istniała odpowiedź.

Co audytor chce zobaczyć.

- zapisane zasady (w Zielonej: polityka, model warstw, nazewnictwo grup `GG_` i `DL_`),
- przykład wniosku o dostęp z zatwierdzeniem właściciela,
- dowód, że ta sama zasada działa w AD, Microsoft 365, Vaultwardenie i aplikacjach.

Jak to mamy w Zielonej. Zasady i katalog wniosków są na stronie Wnioski o usługę, katalog usług i onboarding: od nowego konta do odebrania dostępu, a struktura grup i delegowanie na stronie Struktura OU Zielonej i delegowanie uprawnień. Dowód: wnioski w GLPI z kategorii dostępu.

5.16 Zarządzanie tożsamością: jedno konto, jedna osoba

O co tu naprawdę chodzi. Każda tożsamość (osoba, usługa, urządzenie) ma swój cykl życia od założenia do usunięcia, a konta współdzielone są wyjątkiem z uzasadnieniem [1]. Gdy coś się

stanie, musimy wiedzieć, kto to zrobił, a konto „magazyn” używane przez dziesięć osób to uniemożliwia.

Co audytor chce zobaczyć.

- listę kont z rozróżnieniem: osobowe, administracyjne (`.admin`, `.t0`), usługowe, techniczne,
- uzasadnienie dla każdego konta współdzielonego,
- konta usługowe jako gMSA albo z właścicielem i hasłem w sejfie.

Jak to mamy w Zielonej. Trzy konta na administratora i zasady kont usługowych opisuje Hartowanie Active Directory: model warstw, konta uprzywilejowane, protokoły i audyt, a zamianę kont usługowych Konta usługowe MSA i gMSA. Skanery w Swarzędzu logują się kontami urządzeń, a nie wspólnym kontem pracowników (do sprawdzenia przy przeglądzie WMS). Dowód: fiszki „Wyszukanie kont włączonych, nieużywanych od 90 dni” i „Wyeksportowanie włączonych kont”.

5.17 Informacje uwierzytelniające: hasła, klucze i ich wydawanie

O co tu naprawdę chodzi. Hasła, klucze i kody są wydawane, przechowywane i zmieniane w kontrolowany sposób, a ludzie wiedzą, jak z nimi postępować [1]. W praktyce: pierwsze hasło nie idzie mailem, hasła firmowe są w sejfie, a nie w arkuszu, a reset hasła przez telefon wymaga potwierdzenia tożsamości.

Co audytor chce zobaczyć.

- zasady haseł w domenie zgodne z tym, co mówi polityka,
- sejf haseł z kontrolą dostępu i logowaniem dwuetapowym,
- procedurę resetu hasła (oddzwonienie na numer z kadr).

Jak to mamy w Zielonej. Zasady haseł i blokady konta: polityka domeny i PSO (14 znaków, bez wymuszonego wygasania, blokada po 10 próbach), Vaultwarden: sejf na hasła, który trzymamy u siebie z polityką logowania dwuetapowego na stronie Pierwsza konfiguracja: panel admina, organizacja i zaproszenia i zasada 10 ze Standardu pracy administratora Zielonej: zasady na pierwszy dzień. Hasła lokalnych administratorów zmienia LAPS. Dowód: fiszka „Odczyt polityki haseł domeny”.

5.18 Prawa dostępu: przyznanie, przegląd, odebranie

O co tu naprawdę chodzi. Prawa nadajemy, zmieniamy i odbieramy według zasad z 5.15, a co jakiś czas sprawdzamy, czy wciąż są potrzebne [1]. Przegląd uprawnień robi właściciel informacji, a nie administrator, bo tylko on wie, czy Marek nadal potrzebuje dostępu do raportów sprzedaży.

Co audytor chce zobaczyć.

- zapis przeglądu uprawnień z datą, nazwiskiem przeglądającego i decyzjami,
- przykład odebrania uprawnień po przeglądzie,
- dostęp „na chwilę” z datą wygaśnięcia.

Jak to mamy w Zielonej. Przegląd kwartalny: każdy kierownik dostaje z GLPI zadanie z listą członków grup `DL_` swojego działu i potwierdza albo zgłasza zmiany (propozycja kalendarza na stronie o utrzymaniu ISMS). Dostęp czasowy przez `-MemberTimeToLive` i `VALID UNTIL` opisuje strona o wnioskach i onboardingu. Dowód: zadania przeglądu w GLPI i fiszka „Sprawdzenie członkostw czasowych”. Przegląd udziałów działów na `fs01` (eksport uprawnień, zadanie dla kierownika, dowód przed i po) opisuje strona Audyt dostępu do plików na fs01 i kwartalny przegląd uprawnień z właścicielami działów.

6.5 Obowiązki po odejściu albo zmianie stanowiska

O co tu naprawdę chodzi. Gdy ktoś odchodzi albo zmienia dział, odbieramy dostępy i sprzęt, a obowiązki poufności trwają dalej [1]. Razem z 5.11 (zwrot aktywów) to najczęstsze źródło niezgodności w małych firmach, bo kadry wiedzą o odejściu, a IT nie.

Co audytor chce zobaczyć.

- listę odejść z ostatniego roku z kadr i dla każdej osoby zgłoszenie offboardingu z datą wyłączenia konta,
- potwierdzenie zwrotu laptopa, karty i telefonu,
- dowód, że konto było wyłączone najpóźniej ostatniego dnia pracy.

Jak to mamy w Zielonej. Offboarding z listą kontrolną (zapis listy grup, wyłączenie, przeniesienie do `OU=Wylaczone`, odebranie grup) jest na stronie o wnioskach i onboardingu; odbiór sprzętu opisuje Ewidencja i utylizacja sprzętu w praktyce: NetBox, etykiety QR, protokoły i czyszczenie przed oddaniem. Po scence z panem Wojtkiem dokładamy jedną rzecz: kadry zakładają zgłoszenie offboardingu w GLPI w dniu przyjęcia wypowiedzenia, a nie w dniu odejścia. Dowód: porównanie z listą kadr i zgłoszenia offboardingu.

8.2 Uprawnienia uprzywilejowane: konta, które mogą wszystko

O co tu naprawdę chodzi. Konta z największą władzą są nieliczne, nadawane świadomie, używane tylko do pracy administracyjnej i obserwowane [1]. Przejęcie jednego takiego konta oznacza przejęcie firmy, więc tu audytor patrzy najdokładniej.

Co audytor chce zobaczyć.

- listę członków grup uprzywilejowanych i listę zatwierdzoną, z porównaniem,
- osobne konta administracyjne (nie konto pocztowe z prawami administratora),
- alarm przy zmianie członkostwa w grupie uprzywilejowanej i dowód, że zadziałał.

Jak to mamy w Zielonej. Model warstw, konta `.admin` i `.t0`, puste Domain Admins z członkostwem czasowym, Protected Users i alarmy w Graylogu na zdarzenia 4728, 4732 i 4756 opisuje strona o hartowaniu AD. Dostawca WMS dostaje konto warstwy 1 na czas pracy (ryzyko R-06). Dowód: fiszki „Eksport członków grup uprzywilejowanych” i „Sprawdzenie członkostw czasowych” oraz zapytanie w Graylogu z fiszki na stronie o systemach.

8.3 Ograniczenie dostępu do informacji

O co tu naprawdę chodzi. Dostęp do konkretnych informacji (folderów, baz, raportów) wynika z zasad, a nie z tego, że „wszyscy mają Everyone” [1]. To przełożenie 5.15 na uprawnienia w systemach.

Co audytor chce zobaczyć.

- uprawnienia na udziale `fs01` dla jednego działu, nadane przez grupy, a nie osoby,
- brak uprawnień Everyone albo Authenticated Users z prawem zapisu na danych poufnych,
- uprawnienia w Optimie i WMS przypisane rolom.

Jak to mamy w Zielonej. Udziały i uprawnienia NTFS na serwerze plików z grupami `DL_Ksiegowosc_RW` i podobnymi. Uprawnienia w Optimie nadaje pani Halina według ról, a my sprawdzamy raz w roku, czy role odpowiadają strukturze działu (do ustalenia z dostawcą Optimy, jak wyeksportować listę).

8.4 Dostęp do kodu źródłowego

O co tu naprawdę chodzi. Kod, narzędzia do budowania i biblioteki są dostępne do odczytu i zapisu tylko dla osób, które go potrzebują, a każda zmiana zostawia ślad [1]. Kod aplikacji cennika to też informacja firmy, a często zawiera wiedzę o tym, jak dostać się do baz.

Co audytor chce zobaczyć.

- listę osób z prawem zapisu do repozytoriów, potwierdzoną przez właściciela,
- ochronę gałęzi głównej (zmiany przez przegląd, a nie bezpośredni zapis),
- brak haseł w repozytoriach.

Jak to mamy w Zielonej. Gitea z logowaniem z AD (Logowanie kontem z Active Directory) i zespołami organizacji; hasła poza repozytorium według strony Hasła i sekrety poza repozytorium: .env, Docker secrets i Vaultwarden. Ochronę gałęzi i skanowanie sekretów opisuje strona o zmianach i wytwarzaniu. Dowód: fiszka „Przegląd dostępu do kodu w Gitea”.

8.5 Bezpieczne uwierzytelnianie

O co tu naprawdę chodzi. Sposób logowania jest tak mocny, jak wymaga tego ryzyko systemu: dostęp z internetu i konta uprzywilejowane dostają drugi składnik, a błędne próby są ograniczane [1]. Hasło samo w sobie nie wystarcza do poczty, VPN ani konsoli chmury.

Co audytor chce zobaczyć.

- MFA dla dostępu zdalnego, poczty w chmurze i kont administracyjnych,
- blokadę konta po nieudanych próbach,
- zasady dostępu warunkowego i konta awaryjne z monitoringiem.

Jak to mamy w Zielonej. VPN handlowców z certyfikatem użytkownika (EAP-TLS i FSSO: logowanie do VPN certyfikatem użytkownika i grupami z AD), dostęp warunkowy i MFA w Entra ID (Zasady zgodności i dostęp warunkowy), Protected Users dla kont `.t0`. Według strony o zasadach haseł konta domenowe nie mają jeszcze MFA przy logowaniu do komputerów; to wpis w planie postępowania z ryzykiem, a nie ukryty brak. Dowód: fiszki „Sprawdzenie rejestracji MFA” i „Odczyt polityki haseł domeny”.

8.18 Programy narzędziowe z uprawnieniami

O co tu naprawdę chodzi. Narzędzia, które potrafią obejść zabezpieczenia systemu (konsole administracyjne, edytory rejestru, narzędzia do odczytu pamięci, skanery), są dostępne tylko dla tych, którzy ich potrzebują, i ich użycie jest kontrolowane [1].

Co audytor chce zobaczyć.

- osobną stację administracyjną albo przynajmniej zasady, skąd uruchamiamy narzędzia administracyjne,

- blokadę narzędzi administracyjnych dla zwykłych użytkowników (reguły ASR, ograniczenia PowerShella),
- zapis użycia narzędzi skanujących (PingCastle, skanery podatności) w zgłoszeniach.

Jak to mamy w Zielonej. Osobna stacja administracyjna i raporty PingCastle w zgłoszeniu z ograniczonym dostępem (strona o hartowaniu AD), reguły ASR (strona o politykach Defendera), sudo tylko dla `wheel`. Pytanie o uruchamianie PowerShella przez zwykłych użytkowników zostawiamy do decyzji, bo blokada psuje niektóre skrypty logowania.

5.3 Rozdzielenie obowiązków w dwuosobowym zespole

O co tu naprawdę chodzi. Jedna osoba nie powinna sama zlecać, wykonywać i zatwierdzać czynności, przy której może popełnić błąd albo nadużycie bez wykrycia [1]. W dwuosobowym IT pełny rozdział jest niemożliwy, więc norma oczekuje zabezpieczeń zastępczych.

Co audytor chce zobaczyć.

- kto zatwierdza zmiany i dostępy (nie ta sama osoba, która je wykonuje),
- zapisy, które pozwalają po fakcie sprawdzić pracę administratora (logi, zgłoszenia),
- niezależny przegląd (audyt wewnętrzny, raport dla zarządu).

Jak to mamy w Zielonej. Druga para oczu przy czerwonych kartach i zatwierdzanie zmian przez drugiego administratora (Zmiany, organ zatwierdzający i okna zmian: jak zmieniamy, żeby nic nie zepsuć), wnioski o dostęp zatwierdzane przez właściciela informacji, logi z kontrolerów w Graylogu, do którego administratorzy nie mają prawa kasowania (propozycja do sprawdzenia w konfiguracji ról Grayloga), i audyt wewnętrzny pana Wojtka.

Częste błędy

Objaw	Przyczyna	Co robimy
Konto byłego pracownika działa miesiącami	kadry nie informują IT o odejściu	zgłoszenie offboardingu zakładane przy wypowiedzeniu, porównanie z listą kadr co miesiąc
Lista uprzywilejowanych istnieje, ale nikt jej nie porównuje	eksport bez decyzji	zadanie w GLPI z eksportem, listą zatwierdzoną i komentarzem „zgodne” albo zmianą
Przegląd uprawnień robi administrator	właściciel informacji się wymiguje	przegląd wysyła się kierownikowi, a brak odpowiedzi eskalujemy do pana Zbigniewa

Objaw	Przyczyna	Co robimy
Konto „magazyn” z jednym hasłem na tablicy	wygoda przy zmianach	konta imienne albo konta urządzeń; wyjątek z uzasadnieniem w rejestrze
Hasło startowe wysłane mailem	szybkość	hasło przez telefon albo w Vaultwarden Send z wygaśnięciem, wymuszona zmiana przy pierwszym logowaniu
Dostawca ma stałe konto z prawami administratora	„zawsze tak było”	konto warstwy 1 włączane na czas pracy, wniosek w GLPI, zapis sesji

□□ Ćwiczenia

1. Pan Wojtek pyta, jak udowodnimy, że konto `jan.nowak` nie było używane od 30 czerwca do wyłączenia 19 października. Co pokazujemy?

Odpowiedź

Atrybut `LastLogonDate` z wyniku `Search-ADAccount` (30.06.2026), zapytanie w Graylogu o zdarzenia logowania 4624 i 4625 dla tego konta oraz logi VPN z `fw01` za ten okres. Do tego zgłoszenie w GLPI z wyłączeniem konta i analizą, dlaczego offboarding się nie odbył, czyli działanie korygujące.

1. Ola prosi o prawo zapisu do repozytorium konfiguracji `fw01` w Gitea, „żeby szybciej poprawiać reguły dla swoich aplikacji”. Co odpowiadamy według 8.4 i 5.3?

Odpowiedź

Że zapis do konfiguracji zapory ma tylko zespół IT, a zmiany reguł idą jako wniosek o zmianę w GLPI. Ola może dostać prawo odczytu i proponować zmiany przez pull request, który zatwierdza administrator. Tak zachowujemy rozdział między tym, kto prosi, a tym, kto wykonuje.

1. Dlaczego eksport członków grup uprzywilejowanych zapisujemy z datą w nazwie pliku i dołączamy do zadania w GLPI, zamiast po prostu uruchomić polecenie w dniu audytu?

Odpowiedź

Bo audytor sprawdza, czy kontrola działa przez cały rok, a nie czy w dniu audytu lista jest poprawna. Seria miesięcznych plików z decyzjami w GLPI jest dowodem działania zabezpieczenia; jednorazowy wynik jest tylko zdjęciem stanu.

1. Które z zabezpieczeń tej strony w Zielonej ma dziś najsłabszy dowód i co z tym robimy?

Odpowiedź

8.5 dla logowania do komputerów w domenie: konta domenowe nie mają MFA. Nie ukrywamy tego, tylko wpisujemy do deklaracji stosowania jako „w trakcie” z planem (Windows Hello dla firm albo MFA przy logowaniu przez Intune) i terminem, a ryzyko z tym związane jest w rejestrze z decyzją pana Zbigniewa.

Powiązane: Zabezpieczenia dla IT po ludzku: systemy, sieć i dane · Zabezpieczenia dla IT po ludzku: zmiany, dostawcy, incydenty i ciągłość działania · Skrypty audytowe Active Directory · Windows LAPS: hasło lokalnego administratora w Active Directory · sudo i /etc/sudoers: konfiguracja i audyt · FreeIPA: jedno logowanie dla wszystkich linuksów · Użytkownicy, role i uprawnienia · Jenkins: logowanie kontem z Active Directory · TeamCity: logowanie kontem z Active Directory

Źródła: [1] Parafraza własna sensu zabezpieczeń 5.3, 5.11, 5.15 do 5.18, 6.5, 8.2 do 8.5 i 8.18 na podstawie publicznych opracowań: hightable.io, „ISO 27001 Annex A controls reference guide”; isms.online, opisy zabezpieczeń Załącznika A 2022; advisera.com, baza wiedzy ISO 27001. · [2] Numeracja i nazwy według ISO/IEC 27001:2022 Załącznik A (katalog iso.org), nazwy przetłumaczone własnymi słowami. · Polecenia: Microsoft Learn, moduł ActiveDirectory (Get-ADGroupMember, Get-ADGroup z -ShowMemberTimeToLive, Search-ADAccount, Get-ADUser, Get-ADDefaultDomainPasswordPolicy); man getent. · Ścieżka „User registration details”: Microsoft Learn, Authentication methods activity (nazwy menu do sprawdzenia w portalu, październik 2026). · Wyniki w przykładach: dane świata Zielonej, zgodne z przykładami ze stron o wnioskach i onboardingu oraz o zasadach haseł.

Zabezpieczenia dla IT po ludzku: systemy, sieć i dane

Poziom: średnio

Dotyczy: ISO/IEC 27001:2022 Załącznik A: 8.1, 8.7 do 8.12, 8.15 do 8.17, 8.20, 8.22 do 8.24; Defender for Business, Intune, WSUS, Rocky Linux 9 i 10, Graylog, Zabbix, FortiGate fw01, BitLocker

Czas: ~45 min

Druga strona o zabezpieczeniach dla IT obejmuje to, co dzieje się na serwerach, stacjach i w sieci: ochronę przed złośliwym oprogramowaniem, łatki, konfigurację, logi, monitorowanie, czas, sieć, filtrowanie stron, kryptografię oraz trzy nowe zabezpieczenia o danych: usuwanie, maskowanie i zapobieganie wyciekom. Przy każdym jest odsyłacz do strony, na której to zrobiliśmy, a w Fiszce polecenia, które dają dowód.

Sens zabezpieczeń parafrazujemy na podstawie publicznych opracowań [1][2]. Sześć z czternastu zabezpieczeń na tej stronie jest nowych w wydaniu 2022: 8.9, 8.10, 8.11, 8.12, 8.16 i 8.23. Oznaczamy je w nagłówku słowami „nowe w 2022”.

Skróty użyte na tej stronie (24)

Skrót	Co znaczy
AD	Active Directory: katalog Microsoftu z kontami użytkowników, komputerów i grup w firmie
AI	Artificial Intelligence: sztuczna inteligencja, czyli programy naśladujące ludzkie rozumowanie
CLI	Command Line Interface: praca przez wpisywanie komend w terminalu
DLP	Data Loss Prevention: zapobieganie wyciekom danych, czyli środki, które wykrywają albo blokują wyprowadzenie informacji poufnej poza firmę (nośniki USB, poczta, chmury)
EDR	Endpoint Detection and Response: ochrona stacji, która obserwuje zachowanie programów, nie tylko sygnatury
FAQ	Frequently Asked Questions: zbiór najczęściej zadawanych pytań z odpowiedziami
GLPI	Gestionnaire Libre de Parc Informatique: otwarty system do zgłoszeń, inwentarza i bazy wiedzy IT; w Zielonej działa w kontenerze na docker01
GPO	Group Policy Object: zestaw ustawień wypychanych z Active Directory na komputery

Skrót	Co znaczy
HTML	HyperText Markup Language: format tekstowy stron WWW, tu używany jako format raportu GPO do przeglądania w przeglądarce
IPsec	Internet Protocol Security: zestaw protokołów szyfrujących i uwierzytelniających ruch sieciowy, na nim stoi tunel VPN typu IKEv2
ISMS	Information Security Management System: system zarządzania bezpieczeństwem informacji, czyli polityka, role, ocena ryzyka, cele, pomiar, audyt i doskonalenie, które decydują o zabezpieczeniach i sprawdzają, czy działają
ISO	International Organization for Standardization: organizacja, która wydaje normy techniczne używane na całym świecie
IT	Information Technology: dział albo praca związana z komputerami i infrastrukturą firmy
ITIL	Information Technology Infrastructure Library: zbiór dobrych praktyk zarządzania usługami IT, dziś rozwijany przez PeopleCert; wersja 4 od 2019, wersja 5 od 2026
PDC	Primary Domain Controller: rola FSMO (PDC Emulator) pełniąca funkcje historycznie zarezerwowane dla podstawowego kontrolera domeny, dziś głównie synchronizację czasu i zmiany haseł
RHEL	Red Hat Enterprise Linux: komercyjna dystrybucja Linuksa
RODO	Rozporządzenie o Ochronie Danych Osobowych: unijne przepisy o tym, jak firmy mogą przetwarzać dane osobowe
SSH	Secure Shell: szyfrowane zdalne logowanie do serwera
TLS	Transport Layer Security: szyfrowanie połączeń, np. w HTTPS
USB	Universal Serial Bus: standard portów i urządzeń podłączanych do komputera, tu pendrive'y i inne nośniki wymienne
VLAN	Virtual LAN: wydzielona logicznie sieć na tym samym sprzęcie
VPN	Virtual Private Network: szyfrowany tunel do sieci firmowej
WMS	Warehouse Management System: system zarządzania magazynem
WSUS	Windows Server Update Services: firmowy serwer aktualizacji Windows

Fiszka

Polecenia Windows wykonujemy w PowerShellu kontem `.admin`, polecenia Linux kontem z `sudo` tam, gdzie to zaznaczono, a polecenia FortiOS w CLI `fw01` przez SSH z VLAN 98 albo VPN administratorów. Wszystkie tylko odczytują stan.

> **□□ TYLKO ODCZYT**

Sprawdzenie ochrony antywirusowej stacji: Get-MpComputerStatus

```
Get-MpComputerStatus | Select-Object AMRunningMode, RealTimeProtectionEnabled,
IsTamperProtected, AntivirusSignatureLastUpdated
```

Dowód do 8.7 na jednej maszynie. Dla całej floty dowodem jest raport w portalu Defender albo raport zgodności w Intune, a to polecenie służy do wyrywkowego sprawdzenia przy audytorze.

Przykład:

```
AMRunningMode RealTimeProtectionEnabled IsTamperProtected AntivirusSignatureLastUpdated
------------- ------------------------ ----------------- ---------------------------
Normal                              True              True 23.10.2026 06:51:08
```

□□ TYLKO ODCZYT

Odczyt ostatnich poprawek Windows: Get-HotFix

```
Get-HotFix -ComputerName NazwaSerwera | Sort-Object InstalledOn -Descending | Select-
Object -First 5 HotFixID, Description, InstalledOn
```

Dowód do 8.8 dla serwera Windows: data ostatniej poprawki pokazuje, czy serwer był w oknie aktualizacji. Pełny obraz floty daje raport Intune albo WSUS.

Przykład:

```
HotFixID  Description     InstalledOn
--------  -----------     -----------
KB5066xxx Security Update 20.10.2026 00:00:00
```

□□ **WSUS** = Windows Server Update Services: firmowy serwer aktualizacji Windows

□□ TYLKO ODCZYT

Sprawdzenie oczekujących poprawek bezpieczeństwa na Rocky Linux: dnf updateinfo

```
sudo dnf updateinfo list --security
```

Pokazuje biuletyny bezpieczeństwa, które dotyczą zainstalowanych pakietów, a jeszcze nie są wgrane. Na Rocky Linux 9 to polecenie dnf4, na RHEL 10 i Rocky 10 działa jako alias polecenia `dnf advisory list --security` z dnf5. Pusta lista dzień po oknie aktualizacji to dowód do 8.8.

Przykład:

```
RLSA-2026:xxxx Important/Sec. openssl-libs-3.2.2-xx.el9_6.x86_64
```

RHEL = Red Hat Enterprise Linux: komercyjna dystrybucja Linuksa · **dnf** = Dandified YUM: menedżer pakietów RHEL/Rocky

KLIKAMY W INTERFEJSIE

Przegląd podatności floty: Defender, Vulnerability management

```
security.microsoft.com → Endpoints → Vulnerability management → Weaknesses → filtr: Exploited, Critical
```

Lista podatności z liczbą urządzeń i informacją, czy luka jest wykorzystywana w atakach. Comiesięczny eksport do zadania w GLPI to dowód, że podatności śledzimy, a nie tylko łatamy na ślepo. Szczegóły na stronie o podatnościach w książce o Defenderze.

GLPI = Gestionnaire Libre de Parc Informatique: otwarty system do zgłoszeń, inwentarza i bazy wiedzy IT; w Zielonej działa w kontenerze na docker01

TYLKO ODCZYT

Sprawdzenie dryfu konfiguracji serwerów: ansible-playbook --check --diff

```
ansible-playbook -i NazwaInwentarza NazwaPlaybooka.yml --check --diff
```

Dowód do 8.9 (nowe w 2022): uruchomienie bez zmian pokazuje, czym serwery różnią się od konfiguracji wzorcowej w repozytorium. Pusta lista różnic znaczy, że konfiguracja jest pod kontrolą.

ansible-playbook = uruchom scenariusz Ansible

TYLKO ODCZYT

Wygenerowanie raportu wszystkich zasad grupy: Get-GPOReport

```
Get-GPOReport -All -ReportType Html -Path "C:\IT\Audyt\gpo-$(Get-Date -Format yyyy-MM-dd).html"
```

Dowód do 8.9 dla Windows: jeden plik HTML z ustawieniami wszystkich GPO w domenie. Porównanie z plikiem sprzed kwartału pokazuje zmiany, które powinny mieć numery w GLPI.

HTML = HyperText Markup Language: format tekstowy stron WWW, tu używany jako format raportu GPO do przeglądania w przeglądarce · **GPO** = Group Policy Object: zestaw ustawień wypychanych z Active Directory na komputery · **GLPI** = Gestionnaire Libre de Parc Informatique: otwarty system do zgłoszeń, inwentarza i bazy wiedzy IT; w Zielonej działa w kontenerze na docker01 · **IT** = Information Technology: dział albo praca związana z komputerami i infrastrukturą firmy

TYLKO ODCZYT

Wyszukanie zmian w grupach uprzywilejowanych w Graylogu: EventID

```
EventID:4728 OR EventID:4732 OR EventID:4756
```

Wpisane w wyszukiwarkę Grayloga (strumień `ad-logowania`, zakres: ostatni kwartał) pokazuje każde dodanie konta do grupy. Dowód do 8.15 i 8.16, a razem z eksportem z poprzedniej strony także do 8.2.

TYLKO ODCZYT

Sprawdzenie retencji logów: System, Indices

```
logi.zielona.example → System → Indices → zestaw indeksów → Rotation & Retention
```

Dowód do 8.15: jak długo trzymamy logi. Wartość porównujemy z tym, co zapisaliśmy w polityce i w rejestrze wymagań prawnych; logi, które giną po 7 dniach, nie pozwolą zbadać incydentu wykrytego po miesiącu.

KLIKAMY W INTERFEJSIE

Przegląd aktywnych alarmów: Zabbix, Problems

```
zabbix.zielona.example → Monitoring → Problems → filtr: Severity od High
```

Dowód do 8.16 (nowe w 2022): aktywne problemy i historia ich obsługi. Audytor zwykle prosi o jeden alarm z przeszłości i zgłoszenie w GLPI, które z niego powstało.

GLPI = Gestionnaire Libre de Parc Informatique: otwarty system do zgłoszeń, inwentarza i bazy wiedzy IT; w Zielonej działa w kontenerze na docker01

TYLKO ODCZYT

Sprawdzenie synchronizacji czasu w Windows: w32tm /query /status

```
w32tm /query /status
```

Dowód do 8.17 na kontrolerze z rolą PDC Emulator: źródło czasu i ostatnia udana synchronizacja. Pozostałe maszyny w domenie biorą czas z kontrolerów.

Przykład:

```
Leap Indicator: 0(no warning)
Stratum: 3 (secondary reference - syncd by (S)NTP)
Last Successful Sync Time: 23.10.2026 08:14:02
Source: 0.pl.pool.ntp.org,0x8
```

PDC = Primary Domain Controller: rola FSMO (PDC Emulator) pełniąca funkcje historycznie zarezerwowane dla podstawowego kontrolera domeny, dziś głównie synchronizację czasu i zmiany haseł · **w32tm** = Windows Time: konfiguracja i diagnostyka usługi czasu, np. źródła NTP na PDC Emulator

TYLKO ODCZYT

Sprawdzenie synchronizacji czasu w Linuksie: chronyc tracking

```
chronyc tracking
```

Dowód do 8.17 na serwerze Rocky Linux: źródło czasu, odchylenie i stan synchronizacji. Odchylenie liczone w milisekundach jest w porządku, w sekundach już nie.

Przykład:

```
Reference ID    : 0A140A0B (dc01.ad.zielona.example)
Stratum         : 4
System time     : 0.000312 seconds fast of NTP time
Leap status     : Normal
```

chronyc = chrony client: stan synchronizacji zegara

TYLKO ODCZYT

Odczyt polityk zapory: show firewall policy

```
show firewall policy
```

Dowód do 8.20 i 8.22 w CLI FortiOS na `fw01`: wszystkie polityki z adresami, usługami i logowaniem. Raz na kwartał przeglądamy listę z właścicielami reguł; reguła bez właściciela i bez ruchu trafia do usunięcia przez zmianę.

CLI = Command Line Interface: praca przez wpisywanie komend w terminalu · **show** = FortiOS: wypisuje konfigurację, w podstawowej postaci tylko ustawienia różniące się od domyślnych, a z wariantem full-configuration także wartości domyślne

TYLKO ODCZYT

Odczyt profili filtrowania stron: show webfilter profile

```
show webfilter profile
```

Dowód do 8.23 (nowe w 2022) w CLI FortiOS: które kategorie stron blokujemy. Na laptopach poza siecią firmy to samo robi filtrowanie treści w Defenderze.

CLI = Command Line Interface: praca przez wpisywanie komend w terminalu · **show** = FortiOS: wypisuje konfigurację, w podstawowej postaci tylko ustawienia różniące się od domyślnych, a z wariantem full-configuration także wartości domyślne

TYLKO ODCZYT

Sprawdzenie szyfrowania dysku: manage-bde -status

```
manage-bde -status C:
```

Dowód do 8.1 i 8.24 na laptopie: czy dysk jest zaszyfrowany i jakim algorytmem. Dla całej floty dowodem jest raport szyfrowania w Intune.

Przykład:

```
Conversion Status:    Fully Encrypted
Percentage Encrypted: 100,0%
```

```
Encryption Method:    XTS-AES 128
Protection Status:    Protection On
```

□□ **manage-bde** = BitLocker Drive Encryption: zarządzanie szyfrowaniem dysków

□□ TYLKO ODCZYT

Sprawdzenie ważności certyfikatu usługi: openssl s_client i x509

```
openssl s_client -connect NazwaHosta:443 -servername NazwaHosta </dev/null | openssl x509 -noout -subject -enddate
```

Dowód do 8.24: kto wystawił certyfikat i kiedy wygasa. Zabbix sprawdza to samo automatycznie, a to polecenie służy do pokazania na żywo.

Przykład:

```
subject=CN = pomoc.zielona.example
notAfter=Mar 14 10:12:44 2027 GMT
```

□□ **openssl** = zestaw narzędzi do certyfikatów i szyfrowania

□□ ZMIENIA SYSTEM

Odczyt zasad kryptograficznych systemu: update-crypto-policies --show

```
update-crypto-policies --show
```

Na Rocky Linux pokazuje, jaki zestaw zasad kryptograficznych obowiązuje w całym systemie (na przykład `DEFAULT`). Wynik wpisujemy do standardu konfiguracji serwera jako część 8.24.

□□ **update-crypto-policies** = RHEL i Rocky Linux: pokazuje (--show) albo ustawia zestaw zasad kryptograficznych obowiązujący w całym systemie, np. DEFAULT

□□ TYLKO ODCZYT

Wyszukanie kont wyłączonych do usunięcia: Get-ADUser -SearchBase OU=Wylaczone

```
Get-ADUser -SearchBase "OU=Wylaczone,OU=Uzytkownicy,DC=ad,DC=zielona,DC=example" -Filter * -Properties whenChanged, Description | Where-Object { $_.whenChanged -lt (Get-Date).AddDays(-180) } | Select-Object SamAccountName, whenChanged, Description
```

Dowód do 8.10 (nowe w 2022): konta wyłączone dawniej niż 180 dni temu, które według naszej zasady retencji (propozycja) usuwamy przez zmianę standardową. Okres 180 dni to propozycja do zatwierdzenia z kadrami.

OU = Organizational Unit: folder w Active Directory grupujący konta i komputery · **DC** = Domain Controller: serwer, który trzyma Active Directory i loguje użytkowników

TYLKO ODCZYT

Sprawdzenie maskowania w bazie testowej: SELECT

```
SELECT count(*) AS niezamaskowane FROM NazwaTabeli WHERE NazwaKolumnyEmail NOT LIKE '%@test.zielona.example';
```

> (gdzie `NazwaTabeli` to tabela z danymi klientów w kopii testowej, a `NazwaKolumnyEmail` to kolumna z adresem)

Dowód do 8.11 (nowe w 2022): w kopii testowej bazy aplikacji wszystkie adresy klientów są podmienione na testowe. Wynik różny od zera znaczy, że prawdziwe dane osobowe trafiły do środowiska testowego.

KLIKAMY W INTERFEJSIE

Kontrolowanie nośników wymiennych: Intune, Device control

```
intune.microsoft.com → Endpoint security → Attack surface reduction → Device control → polityka „Zielona: nośniki USB”
```

Dowód do 8.12 (nowe w 2022): zasada, która blokuje zapis na nośniki USB poza urządzeniami z listy dozwolonych. Nazwę polityki proponujemy; ścieżkę menu sprawdzamy w portalu.

ZRZUT EKRANU DO UZUPEŁNIENIA

Zrzut do uzupełnienia: ekran Device control w Intune z polityką „Zielona: nośniki USB”, widoczne przypisanie do grupy komputerów i stan wdrożenia.

USB = Universal Serial Bus: standard portów i urządzeń podłączanych do komputera, tu pendrive'y i inne nośniki wymienne

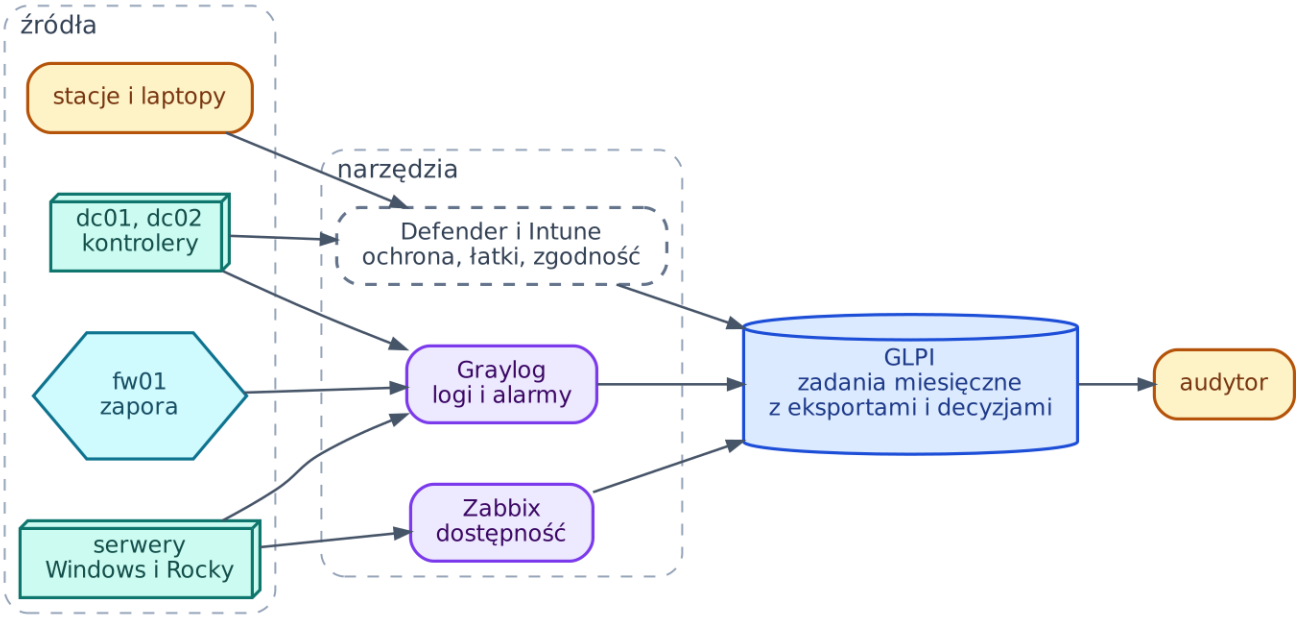
Z życia wzięte

Z ŻYCIA WZIĘTE

Środa, 21 października 2026, 13:15. Pan Wojtek odtwarza z Tomkiem próbę logowania z zewnątrz z ubiegłego tygodnia: w logach `fw01` połączenie VPN jest o 22:03, a nieudane logowanie na `dc01` o 21:59, czyli „przed” połączeniem. Tomek przez kwadrans szuka drugiego intruza, aż starszy administrator sprawdza `w32tm /query /status` na `dc01`: kontroler od aktualizacji hosta brał czas z Hyper-V i spóźniał się o cztery minuty. Pan Wojtek zapisuje to jako przykład, dlaczego 8.17 nie jest drobiazgiem: bez wspólnego czasu nie da się złożyć historii incydentu.

Jak to działa

Zabezpieczenia z tej strony mają jedną wspólną cechę: działają same, w tle, a ślad zostawiają w kilku narzędziach naraz. Audytor nie chce zobaczyć ekranu konfiguracji, tylko dowód, że zabezpieczenie działało przez cały rok i że ktoś reagował, gdy przestało.



Rysunek 1. Skąd biorą się dowody dla zabezpieczeń technologicznych: kontrolery, serwery, stacje i fw01 wysyłają logi do Grayloga i dane do Zabbixa, stacje raportują do Defendera i Intune, a miesięczne zadania w GLPI zbierają eksporty i decyzje, z których korzysta audytor (kliknięcie otwiera pełny rozmiar)

> **Pojęcie: dowód działania zabezpieczenia.** Zapis, który pokazuje, że zabezpieczenie działało w przeszłości, a nie tylko, że jest skonfigurowane dziś. Dla kopii to protokoły testów z kilku kwartałów, dla łatek raporty z kilku miesięcy, dla logów alarm z przeszłości i zgłoszenie, które z niego powstało.

W Zielonej dowody zbiera jedno zadanie cykliczne w GLPI na każdy miesiąc, „Przegląd ISMS: dowody miesięczne” (propozycja), z listą kontrolną: eksport uprzywilejowanych, porównanie kont z kadrami, raport podatności, raport łatek, test pliku z kopii, przegląd alarmów. Wynik każdego punktu to załącznik albo komentarz z decyzją.

Zabezpieczenia po kolei

8.1 Urządzenia końcowe użytkowników

O co tu naprawdę chodzi. Laptopy, komputery i telefony służbowe są skonfigurowane i chronione tak, żeby ich zgubienie albo przejęcie nie otwierało drogi do informacji firmy [1].

Co audytor chce zobaczyć.

- raport zgodności floty: szyfrowanie, aktualny system, ochrona antywirusowa,
- procedurę po zgubieniu laptopa (zdalne wyczyszczenie, wyłączenie dostępu),
- zasady dla urządzeń prywatnych, jeśli dopuszczamy dostęp z nich.

Jak to mamy w Zielonej. Zasady zgodności i dostęp warunkowy, BitLocker z Intune: ciche szyfrowanie i klucze odzyskiwania w Entra ID, zdalne akcje na stronie o aktualizacjach i raportach Intune oraz Urządzenia służbowe i prywatne: BYOD, COPE, COBO. Dowód: raport zgodności w Intune i fiszka „Sprawdzenie szyfrowania dysku".

8.7 Ochrona przed złośliwym oprogramowaniem

O co tu naprawdę chodzi. Na każdym systemie, gdzie to ma sens, działa ochrona przed złośliwym oprogramowaniem, a ludzie wiedzą, czego nie otwierać [1]. Sam antywirus nie wystarcza: liczą się też ograniczenia uruchamiania i szkolenie.

Co audytor chce zobaczyć.

- pokrycie: lista urządzeń z agentem i bez niego, z wyjaśnieniem wyjątków,
- aktualne sygnatury i włączoną ochronę przed manipulacją,
- przykład alertu i jego obsługi.

Jak to mamy w Zielonej. Defender for Business na stacjach i serwerach Windows (Polityki ochrony: ochrona nowej generacji, zapora, reguły ASR i kontrolowany dostęp do folderów), agent na serwerach linuksowych (Agent ochrony na serwerach Linux: instalacja i weryfikacja), obsługa alertów na stronie o incydentach i EDR. Dowód: fiszka „Sprawdzenie ochrony antywirusowej" i incydent z kolejki Defendera z numerem w GLPI.

8.8 Zarządzanie podatnościami technicznymi

O co tu naprawdę chodzi. Wiemy, jakie mamy oprogramowanie, dowiadujemy się o jego lukach, oceniamy je i łatamy w rozsądnym czasie, zaczynając od najgroźniejszych [1].

Co audytor chce zobaczyć.

- zapisane czasy łatania według wagi (na przykład krytyczne wykorzystywane w atakach w 7 dni),
- raporty z kilku miesięcy pokazujące, że czasy są dotrzymywane,

- wyjątki z uzasadnieniem (system, którego nie da się załatać, i co robimy zamiast).

Jak to mamy w Zielonej. Zarządzanie podatnościami i raporty: co łatać najpierw, Aktualizacje Windows i raporty: pierścienie, Autopatch, zgodność floty, Standardowa aktualizacja systemu produkcyjnego (Windows) i dnf: instalacja, aktualizacja, historia, wycofywanie zmian. Wyjątkiem jest `syb01` ze starym systemem płacowym, którego nie łatamy do nowych wersji; zamiast tego jest odcięty od internetu i dostępny tylko do odczytu (do potwierdzenia w konfiguracji `fw01`). Dowód: fiszki o poprawkach i raport podatności.

8.9 Zarządzanie konfiguracją (nowe w 2022)

O co tu naprawdę chodzi. Konfiguracje sprzętu, systemów, usług i sieci, także ustawienia bezpieczeństwa, są ustalone, zapisane, wdrażane w powtarzalny sposób, pilnowane i zmieniane tylko przez proces zmian [1][3]. Serwer postawiony „z ręki” przez Tomka w piątek jest niezgodny z tym zabezpieczeniem, nawet jeśli działa.

Co audytor chce zobaczyć.

- wzorcowe konfiguracje (szablony, playbooki, GPO, profile Intune) w repozytorium albo narzędziu,
- sposób wykrywania odchyleń od wzorca,
- powiązanie zmian konfiguracji z numerami zmian.

Jak to mamy w Zielonej. Konfiguracje w Gitea z numerami zmian w commitach (strona o zmianach w książce o ITIL), Ansible dla linuksów (Ansible: podstawy operacyjne), GPO i profile Intune (Profile konfiguracji: katalog ustawień zamiast GPO), kopia konfiguracji `fw01` co noc (strona o strategii kopii). Dowód: fiszki „Sprawdzenie dryfu konfiguracji” i „Wygenerowanie raportu wszystkich zasad grupy”.

8.15 Logowanie zdarzeń

O co tu naprawdę chodzi. Systemy zapisują zdarzenia ważne dla bezpieczeństwa (logowania, zmiany uprawnień, błędy, działania administratorów), zapisy są chronione przed zmianą i przechowywane tak długo, jak trzeba, a ktoś je czyta [1].

Co audytor chce zobaczyć.

- listę źródeł logów i tego, co z nich zbieramy,
- retencję i ochronę logów przed skasowaniem przez administratora systemu, z którego pochodzą,

- przykład wyszukania zdarzenia sprzed kilku tygodni.

Jak to mamy w Zielonej. Graylog (Po co centralne logowanie i jak to działa, Wysyłka logów z hostów, Graylog: codzienna praca z logami), zakres audytu kontrolerów na stronie o hartowaniu AD , na linuksach Audyt i ślady logowań: auditd, last, lastb, journalctl. Dowód: fiszki o Graylogu.

8.16 Monitorowanie działań (nowe w 2022)

O co tu naprawdę chodzi. Sieć, systemy i aplikacje są obserwowane pod kątem nietypowego zachowania, a wykryte anomalie oceniamy i w razie potrzeby traktujemy jak incydent [1][3]. Logi z 8.15 to zapis, monitorowanie to ktoś albo coś, co na ten zapis patrzy i reaguje.

Co audytor chce zobaczyć.

- definicje alarmów (co uznajemy za nietypowe: logowanie administratora w nocy, seria nieudanych logowań, dodanie do grupy),
- kanał powiadomień i dowód reakcji na alarm,
- przegląd alarmów fałszywych i strojenie.

Jak to mamy w Zielonej. Alarmy w Graylogu (definicje zdarzeń i powiadomienia na stronie o codziennej pracy z Graylogiem), Zabbix dla dostępności i wydajności (Host, element danych, wyzwalacz, akcja: jak to się składa), EDR w Defenderze. Alarm z wagą High i wyżej staje się zgłoszeniem w GLPI (strona o incydentach). Dowód: fiszka „Przegląd aktywnych alarmów” i jedno zgłoszenie z alarmu.

8.17 Synchronizacja zegarów

O co tu naprawdę chodzi. Wszystkie systemy biorą czas z tego samego, zatwierdzonego źródła, żeby zdarzenia z różnych logów dało się ułożyć w jedną historię [1].

Co audytor chce zobaczyć.

- zapisane źródło czasu (w Zielonej: PDC Emulator synchronizowany z publicznym źródłem, reszta domeny z kontrolerów, linuksy z kontrolerów przez chrony),
- wyrywkowe sprawdzenie kilku systemów, w tym `fw01`,
- alarm przy rozjechaniu czasu.

Jak to mamy w Zielonej. Kontrolery w utrzymaniu: replikacja, FSMO, trzeci kontroler i wycofanie z konfiguracją czasu PDC i Synchronizacja czasu: chrony, timedatectl. PDC Emulator na `dc01` bierze

czas z polskiej puli `0.pl.pool.ntp.org` i `1.pl.pool.ntp.org`, tak jak ustawia go fiszka na stronie o kontrolerach. Dowód: fiszki o czasie.

8.20 Bezpieczeństwo sieci i 8.22 rozdzielenie sieci

O co tu naprawdę chodzi. Sieć i urządzenia sieciowe są zarządzane i chronione, a grupy systemów i użytkowników o różnym poziomie zaufania są w osobnych sieciach z kontrolowanym ruchem między nimi [1].

Co audytor chce zobaczyć.

- aktualny schemat sieci z VLAN-ami i strefami,
- reguły zapory między strefami z właścicielami i przeglądem,
- dostęp administracyjny do urządzeń sieciowych tylko z wydzielonej sieci.

Jak to mamy w Zielonej. VLAN-y serwerów, biura, magazynu, zarządzania, kamer i gości ze strony o świecie Zielonej, FortiGate w zarządzaniu siecią: interfejsy, VLAN-y, polityki i NAT, zarządzanie urządzeniami tylko z VLAN 98 i VPN administratorów, NetBox jako aktualny opis sieci. Dowód: fiszka „Odczyt polityk zapory” i protokół kwartalnego przeglądu reguł.

8.23 Filtrowanie stron internetowych (nowe w 2022)

O co tu naprawdę chodzi. Dostęp do stron zewnętrznych jest ograniczany tak, żeby pracownicy nie trafiali na strony ze złośliwym oprogramowaniem, wyłudzające dane albo niezgodne z zasadami firmy [1][3].

Co audytor chce zobaczyć.

- zasady: jakie kategorie blokujemy i dlaczego,
- działanie także poza siecią firmy (laptopy handlowców),
- obsługę wyjątków (wniosek o odblokowanie strony).

Jak to mamy w Zielonej. Profil filtrowania stron na `fw01` dla ruchu z biura i magazynu oraz ochrona sieci i filtrowanie treści w Defenderze dla laptopów (sekcja o ochronie sieci na stronie o politykach Defendera). Wyjątki przez wniosek w GLPI. Dowód: fiszka „Odczyt profili filtrowania stron” i raport filtrowania treści w portalu Defender.

8.24 Używanie kryptografii

O co tu naprawdę chodzi. Firma ma zasady, gdzie szyfrujemy (dyski, połączenia, kopie), jakimi algorytmami i jak zarządzamy kluczami przez cały ich cykl życia [1]. Najczęściej zapomnianą częścią jest właśnie zarządzanie kluczami: kto ma klucz odzyskiwania i co się stanie, gdy go zgubimy.

Co audytor chce zobaczyć.

- listę: co szyfrujemy, czym i gdzie leżą klucze,
- kontrolę ważności certyfikatów,
- procedurę odzyskania klucza i jej test.

Jak to mamy w Zielonej. BitLocker z kluczami w Entra ID i AD, TLS z certyfikatami z `CA-Zielona` i publicznymi (Certyfikaty SSL: wystawienie, konwersja, weryfikacja, TLS w Nginx), szyfrowanie kopii restic i klucze w sejfie (sekcja „Szyfrowanie i klucze” na stronie o strategii kopii), VPN IPsec z certyfikatami. Dowód: fiszki o szyfrowaniu, certyfikacie i zasadach kryptograficznych.

> Po przenosinach urzędu według strony Przenosiny urzędu z dc01 bez przerwy: dwa urzędy równolegle i wygaszenie CA-Zielona nowe certyfikaty wystawia `Zielona-CA01` na `ca01`, więc wszędzie, gdzie dziś ufamy tylko `CA-Zielona`, dokładamy zaufanie do `Zielona-Root-CA`.

8.10 Usuwanie informacji (nowe w 2022)

O co tu naprawdę chodzi. Informacje, które nie są już potrzebne, usuwamy ze wszystkich miejsc, gdzie leżą (systemy, kopie, nośniki, usługi dostawców), w sposób dopasowany do ich wrażliwości, i umiemy to pokazać [1][3]. To zabezpieczenie spotyka się z RODO: dane osobowe przechowywane dłużej niż trzeba to też naruszenie.

Co audytor chce zobaczyć.

- zasady retencji dla głównych rodzajów informacji,
- protokoły niszczenia albo kasowania nośników,
- przykład usunięcia danych po upływie okresu, także u dostawcy chmury.

Jak to mamy w Zielonej. Okresy przechowywania i retencja kopii na stronie Strategia kopii zapasowych Zielonej: RPO, RTO, reguła 3-2-1-1-0 i dwie lokalizacje, niszczenie nośników z protokołem (Niszczenie nośników: DIN 66399, kasowanie dysków i protokół), czyszczenie sprzętu przed oddaniem na stronie o ewidencji i utylizacji. Brakuje zapisanej zasady usuwania kont wyłączonych; proponujemy 180 dni. Dowód: fiszka „Wyszukanie kont wyłączonych do usunięcia” i protokoły niszczenia.

8.11 Maskowanie danych (nowe w 2022)

O co tu naprawdę chodzi. Tam, gdzie pełne dane nie są potrzebne (testy, raporty, szkolenia, wsparcie dostawcy), dane osobowe i wrażliwe są ukryte, zastąpione albo zanonimizowane [1][3].

Co audytor chce zobaczyć.

- zasadę, że do środowisk testowych nie trafiają prawdziwe dane osobowe albo trafiają zamaskowane,
- skrypt albo procedurę maskowania,
- sprawdzenie, że maskowanie zadziałało.

Jak to mamy w Zielonej. Zespół Oli testuje aplikacje na kopiach baz z `pg01` i `my01`; po scence z tej strony proponujemy krok maskowania jako część procedury odświeżania bazy testowej (skrypt w repozytorium aplikacji, właściciel Ola). Optima i WMS nie mają środowisk testowych z kopią produkcji (do potwierdzenia z panią Haliną i Markiem). Dowód: fiszka „Sprawdzenie maskowania w bazie testowej”.

8.12 Zapobieganie wyciekom danych (nowe w 2022)

O co tu naprawdę chodzi. Firma ogranicza drogi, którymi informacja poufna może wyjść na zewnątrz bez zgody: nośniki wymienne, poczta, prywatne chmury, wydruki, schowek do narzędzi AI [1][3]. Zabezpieczenie nie wymaga drogiego systemu DLP (Data Loss Prevention), tylko rozsądnych środków dopasowanych do ryzyka.

Co audytor chce zobaczyć.

- wiedzę, gdzie są dane poufne (klasyfikacja i rejestr informacji),
- zablokowane albo kontrolowane główne kanały wycieku,
- obsługę zdarzeń: co się dzieje, gdy blokada zadziała.

Jak to mamy w Zielonej. Klasyfikacja i rejestr informacji na stronie o zakresie i ryzyku, kontrola nośników USB w Intune (propozycja), Polityka użycia AI w firmie: wzór dla Zielonej dla narzędzi AI, filtrowanie stron z 8.23 dla prywatnych usług przechowywania plików. Funkcje DLP w Microsoft Purview z pakietu Business Premium obejmują usługi Microsoft 365, a nie pocztę w MailCow; zakres licencji sprawdzamy w dokumentacji Microsoftu przed decyzją (do potwierdzenia). Dowód: fiszka „Kontrolowanie nośników wymiennych”.

Częste błędy

Objaw	Przyczyna	Co robimy

Logi z różnych systemów nie dają się złożyć w jedną historię	rozjechany czas, maszyny wirtualne biorą czas z hosta	jedno źródło czasu, wyłączona synchronizacja czasu z Hyper-V na kontrolerach, alarm w Zabbiksie
Raport łatek jest, czasów łatania nie ma	brak zapisanej zasady	tabela czasów według wagi w procedurze, raport miesięczny z porównaniem
Audytor pyta o konfigurację wzorcową serwera, a jej nie ma	serwery stawiane ręcznie	playbook albo szablon maszyny w repozytorium, odchylenia przez `--check --diff`
Graylog kasuje logi po tygodniu	domyślna retencja zestawu indeksów	retencja zgodna z polityką, sprawdzona fiszką
Prawdziwe dane klientów w bazie testowej	kopia produkcji „na szybko”	maskowanie jako krok procedury odświeżania, sprawdzenie zapytaniem
Filtrowanie stron działa tylko w biurze	filtr wyłącznie na zaporze	filtrowanie treści w Defenderze na laptopach
Nikt nie wie, gdzie są klucze odzyskiwania	szyfrowanie bez zarządzania kluczami	lista kluczy i ich miejsc, test odzyskania raz w roku

□□ Ćwiczenia

1. Audytor prosi o dowód, że krytyczne poprawki na serwerach Windows instalujemy w ciągu 14 dni. Co pokazujemy?

Odpowiedź

Zapisaną zasadę czasów łatania, raporty z kilku miesięcy (Intune albo WSUS dla serwerów, raport podatności z Defendera) i wyrywkowo `Get-HotFix` na dwóch serwerach z datą po trzecim wtorku miesiąca. Jeśli któryś serwer jest wyjątkiem, pokazujemy wpis wyjątku z uzasadnieniem i terminem.

1. Dlaczego 8.15 i 8.16 to dwa różne zabezpieczenia, skoro oba dotyczą Grayloga?

Odpowiedź

8.15 dotyczy zapisywania i przechowywania zdarzeń, 8.16 tego, czy ktoś albo coś na nie patrzy i reaguje na nietypowe zachowanie. Można mieć świetne logi, których nikt nie czyta, i wtedy 8.15 jest spełnione, a 8.16 nie.

1. Ola chce dać dostawcy biblioteki kopię bazy cennika do analizy błędu. Które zabezpieczenia z tej strony wchodzą w grę i co robimy?

Odpowiedź

8.11 (maskowanie: dostawca dostaje kopię z zamaskowanymi danymi osobowymi), 8.12 (kontrolowany kanał przekazania, nie prywatny dysk w chmurze), 8.24 (szyfrowanie paczki) i 8.10 (usunięcie kopii u dostawcy po zakończeniu, z potwierdzeniem). Do tego umowa z dostawcą, czyli zabezpieczenia o dostawcach ze strony o zmianach i dostawcach.

1. W scence `dc01` brał czas z hosta Hyper-V. Gdzie w tej bazie jest opis, jak to naprawić, i jak pokażemy audytorowi, że problem nie wróci?

Odpowiedź

Konfigurację czasu na PDC i wyłączenie synchronizacji czasu z hostem opisuje strona o kontrolerach w utrzymaniu. Żeby problem nie wrócił, dokładamy w Zabbiksie wyzwalacz na różnicę czasu kontrolera względem źródła i pokazujemy audytorowi definicję wyzwalacza oraz zgłoszenie z incydentu jako działanie korygujące.

Powiązane: Zabezpieczenia dla IT po ludzku: dostęp, tożsamość i konta uprzywilejowane · Zabezpieczenia dla IT po ludzku: zmiany, dostawcy, incydenty i ciągłość działania · Alerty, incydenty i EDR: co robimy, gdy Defender coś znajdzie · Retencja i czyszczenie dzienników · SELinux: podstawy, tryby, konteksty · firewalld: strefy, porty, usługi, rich rules

Źródła: [1] Parafraza własna sensu zabezpieczeń 8.1, 8.7 do 8.12, 8.15 do 8.17, 8.20, 8.22 do 8.24 na podstawie publicznych opracowań: hightable.io, „ISO 27001 Annex A controls reference guide”; isms.online, opisy zabezpieczeń Załącznika A 2022; advisera.com, baza wiedzy ISO 27001. · [2] Numery według ISO/IEC 27001:2022 Załącznik A (katalog iso.org). · [3] Lista jedenastu nowych zabezpieczeń 2022: hightable.io (FAQ) i isms.online, „What is Annex A, and what has changed?”. · Polecenia: Microsoft Learn (Get-MpComputerStatus, Get-HotFix, Get-GPOReport, w32tm, manage-bde, Get-ADUser); dnf5.readthedocs.io, „Advisory command” (alias `updateinfo` dla `advisory` w dnf5); dokumentacja chrony (`chronyc tracking`); Fortinet, FortiOS CLI reference (`show firewall policy`, `show webfilter profile`, składnię sprawdzamy w naszej wersji); man openssl-s_client, openssl-x509, update-crypto-policies. · Wyniki w przykładach: dane świata Zielonej, numery biuletynów i poprawek zastąpione znakami `x`, bo nie podajemy wymyślonych numerów.

Zabezpieczenia dla IT po ludzku: zmiany, dostawcy, incydenty i ciągłość działania

Poziom: średnio

Dotyczy: ISO/IEC 27001:2022 Załącznik A: 5.7, 5.19 do 5.30, 6.8, 7.4, 7.14, 8.13, 8.14, 8.25, 8.28, 8.31, 8.32; GLPI, Gitea, restic na bkp01 i bkp02, macierz wysokiej dostępności

Czas: ~45 min

Trzecia strona o zabezpieczeniach dla IT obejmuje to, co dzieje się w czasie: zmiany i wytwarzanie oprogramowania, dostawców i chmurę, informacje o zagrożeniach, incydenty, kopie i ciągłość działania. Prawie wszystko z tej strony Zielona już robi według książek o ITIL, kopiach i wysokiej dostępności, więc głównym zadaniem jest pokazanie dowodów i domknięcie kilku luk.

Sens zabezpieczeń parafrazujemy na podstawie publicznych opracowań [1][2]. Nowe w wydaniu 2022 są tu 5.7, 5.23, 5.30, 7.4 i 8.28.

Skróty użyte na tej stronie (22)

Skrót	Co znaczy
AI	Artificial Intelligence: sztuczna inteligencja, czyli programy naśladujące ludzkie rozumowanie
AWS	Amazon Web Services: chmura Amazonu
CERT	Computer Emergency Response Team: zespół reagowania na incydenty; CERT Polska działa w NASK i publikuje ostrzeżenia o zagrożeniach
CISA	Cybersecurity and Infrastructure Security Agency: amerykańska agencja bezpieczeństwa cyberprzestrzeni, prowadząca wykaz podatności wykorzystywanych w atakach
CSIRT	Computer Security Incident Response Team: zespół reagowania na incydenty komputerowe; w Polsce m.in. CSIRT NASK, CSIRT GOV, CSIRT MON i zespoły sektorowe, do których podmioty kluczowe i ważne zgłaszają incydenty poważne

Skrót	Co znaczy
CVE	Common Vulnerabilities and Exposures: publiczny numer katalogowy konkretnej luki bezpieczeństwa, ten sam numer identyfikuje ją u każdego producenta
GLPI	Gestionnaire Libre de Parc Informatique: otwarty system do zgłoszeń, inwentarza i bazy wiedzy IT; w Zielonej działa w kontenerze na docker01
ICT	Information and Communication Technology: technologie informacyjne i komunikacyjne, czyli systemy, sieci i usługi IT razem z łącznością
ISO	International Organization for Standardization: organizacja, która wydaje normy techniczne używane na całym świecie
IT	Information Technology: dział albo praca związana z komputerami i infrastrukturą firmy
ITIL	Information Technology Infrastructure Library: zbiór dobrych praktyk zarządzania usługami IT, dziś rozwijany przez PeopleCert; wersja 4 od 2019, wersja 5 od 2026
JSON	JavaScript Object Notation: tekstowy format danych z klamrami i cudzysłowami
KEV	Known Exploited Vulnerabilities: wykaz agencji CISA z podatnościami, o których wiadomo, że atakujący naprawdę je wykorzystują
KSC	krajowy system cyberbezpieczeństwa: polska ustawa, od 3 kwietnia 2026 w wersji wdrażającej dyrektywę NIS2, z obowiązkami zgłaszania incydentów
MFA	Multi-Factor Authentication: logowanie drugim składnikiem, np. kodem z telefonu
RODO	Rozporządzenie o Ochronie Danych Osobowych: unijne przepisy o tym, jak firmy mogą przetwarzać dane osobowe
RPO	Recovery Point Objective: ile danych wolno stracić przy awarii
RTO	Recovery Time Objective: jak długo wolno nie działać przy awarii
UODO	Urząd Ochrony Danych Osobowych: polski organ nadzorujący przestrzeganie RODO
UPS	Uninterruptible Power Supply: zasilacz awaryjny, podtrzymuje zasilanie urządzeń na czas zaniku napięcia z sieci
VPN	Virtual Private Network: szyfrowany tunel do sieci firmowej
WMS	Warehouse Management System: system zarządzania magazynem

Fiszka

□□ TYLKO ODCZYT

Wypisanie zmian konfiguracji z kwartału: git log --grep

```
git log --since="3 months ago" --oneline --grep "CHG-"
```

Wykonujemy w klonie repozytorium konfiguracji w Gitea. Dowód do 8.32: każda zmiana pliku ma numer zmiany z GLPI, a numer prowadzi do oceny ryzyka, zatwierdzenia i planu wycofania.

Przykład:

```
3f1c9a2 CHG-0042: GLPI 12.0.0, nowy obraz i MariaDB 11.4.13
9b07e15 CHG-0047: fw01, nowa grupa adresów dla drukarek etykiet
```

GLPI = Gestionnaire Libre de Parc Informatique: otwarty system do zgłoszeń, inwentarza i bazy wiedzy IT; w Zielonej działa w kontenerze na docker01 · **git** = system kontroli wersji (nazwa to brytyjski slang: nieznośny typ)

KLIKAMY W INTERFEJSIE

Wyeksportowanie dziennika zmian z GLPI: Assistance, Changes

```
pomoc.zielona.example → Assistance → Changes → filtr: Date, ostatni kwartał → kolumny:
tytuł, rodzaj, status, zatwierdzający → Export CSV
```

Dowód do 8.32: pełna lista zmian z rodzajem (standardowa, normalna, awaryjna) i zatwierdzeniem. Audytor wybiera z niej dwie albo trzy zmiany i prosi o szczegóły.

GLPI = Gestionnaire Libre de Parc Informatique: otwarty system do zgłoszeń, inwentarza i bazy wiedzy IT; w Zielonej działa w kontenerze na docker01

TYLKO ODCZYT

Sprawdzenie ochrony gałęzi głównej w Gitea: Branch protection

```
git.zielona.example → NazwaRepozytorium → Settings → Branches → Branch protection dla
main → zapis tylko przez pull request, wymagane zatwierdzenie
```

Dowód do 8.25 i 8.28 (nowe w 2022): kod trafia do gałęzi głównej tylko po przeglądzie drugiej osoby. Zrzut ustawień jednego repozytorium aplikacji wystarcza jako przykład.

ZRZUT EKRANU DO UZUPEŁNIENIA

Zrzut do uzupełnienia: ekran Settings → Branches w repozytorium aplikacji cennika w Gitea, widoczna reguła ochrony gałęzi `main` z wymaganym zatwierdzeniem pull requestu.

□□ TYLKO ODCZYT

Skanowanie historii repozytorium pod kątem sekretów: gitleaks git

```
gitleaks git
```

Wykonujemy w katalogu repozytorium. Dowód do 8.28 (nowe w 2022) i 8.4: w historii nie ma haseł ani tokenów. Narzędzie i jego opcje opisuje strona o asystentach kodujących w książce o AI.

□□ **AI** = Artificial Intelligence: sztuczna inteligencja, czyli programy naśladujące ludzkie rozumowanie · **gitleaks** = narzędzie szukające haseł, tokenów i kluczy w plikach i w historii repozytorium Git

□□ KLIKAMY W INTERFEJSIE

Przegląd rejestru dostawców i umów: GLPI, Management

```
pomoc.zielona.example → Management → Suppliers → kolumny: nazwa, rodzaj usługi, umowy → Management → Contracts → daty końca i przeglądu
```

Dowód do 5.19 do 5.22: lista dostawców z umowami i datą ostatniej oceny. Pole „krytyczność” i „ocena bezpieczeństwa” dodajemy jako pola własne albo w opisie (propozycja).

□□ **GLPI** = Gestionnaire Libre de Parc Informatique: otwarty system do zgłoszeń, inwentarza i bazy wiedzy IT; w Zielonej działa w kontenerze na docker01

□□ KLIKAMY W INTERFEJSIE

Przegląd aplikacji chmurowych z logowaniem przez Entra ID: Enterprise applications

```
entra.microsoft.com → Entra ID → Enterprise apps → All applications → kolumny: nazwa, data utworzenia, właściciel
```

Dowód do 5.23 (nowe w 2022): usługi chmurowe, do których logujemy się kontem firmowym. Lista uzupełnia rejestr usług chmurowych o te, które ktoś dodał sam przez zgodę na aplikację.

□□ TYLKO ODCZYT

Wyszukanie nowych wykorzystywanych podatności w naszym sprzęcie: CISA KEV i jq

```
curl -s
https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json | jq
-r '.vulnerabilities[] | select(.vendorProject=="NazwaProducenta") | [.dateAdded,
.cveID, .product] | @tsv' | sort | tail -5
```

> (gdzie `NazwaProducenta` to nazwa producenta w wykazie, np. `Fortinet` albo `Microsoft`)

Dowód do 5.7 (nowe w 2022): pobieramy wykaz podatności wykorzystywanych w atakach i filtrujemy po producentach z NetBoksa. Nowa pozycja dla naszego sprzętu to zgłoszenie w GLPI, a często zmiana awaryjna.

Przykład:

```
2026-10-09□CVE-2026-xxxxx□FortiOS
```

□□ **CISA** = Cybersecurity and Infrastructure Security Agency: amerykańska agencja bezpieczeństwa cyberprzestrzeni, prowadząca wykaz podatności wykorzystywanych w atakach ·**KEV** = Known Exploited Vulnerabilities: wykaz agencji CISA z podatnościami, o których wiadomo, że atakujący naprawdę je wykorzystują · **GLPI** = Gestionnaire Libre de Parc Informatique: otwarty system do zgłoszeń, inwentarza i bazy wiedzy IT; w Zielonej działa w kontenerze na docker01 ·**curl** = client URL: pobieranie i wysyłanie przez HTTP z terminala

□□ **TYLKO ODCZYT**

Sprawdzenie ostatniej kopii w repozytorium: restic snapshots --latest

```
sudo -u restic restic -r /backup/rest/NazwaRepozytorium --password-file
/etc/restic/haslo-NazwaRepozytorium snapshots --latest 1
```

Wykonujemy na `bkp01`. Dowód do 8.13: najnowsza migawka repozytorium z datą i hostem. Razem z protokołami testów odtwarzania to pełny dowód, że kopie powstają i dają się odtworzyć.

□□ **TYLKO ODCZYT**

Wyrywkowe sprawdzenie danych kopii: restic check --read-data-subset

```
sudo -u restic restic -r /backup/rest/NazwaRepozytorium --password-file
/etc/restic/haslo-NazwaRepozytorium check --read-data-subset=5%
```

Dowód do 8.13: repozytorium jest spójne, a losowe 5 procent danych da się odczytać. Wynik cotygodniowej kontroli trafia do logów na serwerze kopii; przy audytorze uruchamiamy polecenie na małym repozytorium.

□□ TYLKO ODCZYT

Wypisanie kopii stanu systemu kontrolera: wbadmin get versions

```
wbadmin get versions -backupTarget:NazwaUdzialu
```

Dowód do 8.13 i 5.30 dla tożsamości: lista kopii stanu systemu kontrolera domeny z datami. Bez tej kopii odtworzenie domeny po ataku na kontrolery trwa dni zamiast godzin.

□□ **wbadmin** = CLI: narzędzie kopii zapasowych Windows, tu do zrobienia spójnej kopii stanu systemu kontrolera domeny

□□ TYLKO ODCZYT

Policzenie sumy kontrolnej zebranego dowodu: sha256sum

```
sha256sum NazwaPlikuDowodu
```

Dowód do 5.28: zaraz po zebraniu logów, obrazu dysku albo eksportu przy incydencie liczymy sumę kontrolną i wpisujemy ją do zgłoszenia z godziną. Późniejsza zgodność sumy pokazuje, że nikt nie zmienił materiału.

Przykład:

```
4b1f0c9e7a2d55e0c3f1b8a6d9e2c7f04a1b3c5d6e7f8091a2b3c4d5e6f70812  security-dc01-2026-10-
21.evtx
```

□□ **sha256sum** = policz skrót SHA256 z pliku albo strumienia wejścia, tu z hasła administratora Graylogu

KLIKAMY W INTERFEJSIE

Zestawienie incydentów bezpieczeństwa z roku: GLPI, filtr kategorii

```
pomoc.zielona.example → Assistance → Tickets → filtr: Category = Incydent bezpieczeństwa, Date: ostatnie 12 miesięcy → kolumny: priorytet, czas zgłoszenia, czas rozwiązania, problem
```

Dowód do 5.24 do 5.27: wszystkie incydenty bezpieczeństwa z oceną, przebiegiem i wnioskami. Kategorię „Incydent bezpieczeństwa” dodajemy w GLPI jako podkategorię incydentów (propozycja).

GLPI = Gestionnaire Libre de Parc Informatique: otwarty system do zgłoszeń, inwentarza i bazy wiedzy IT; w Zielonej działa w kontenerze na docker01

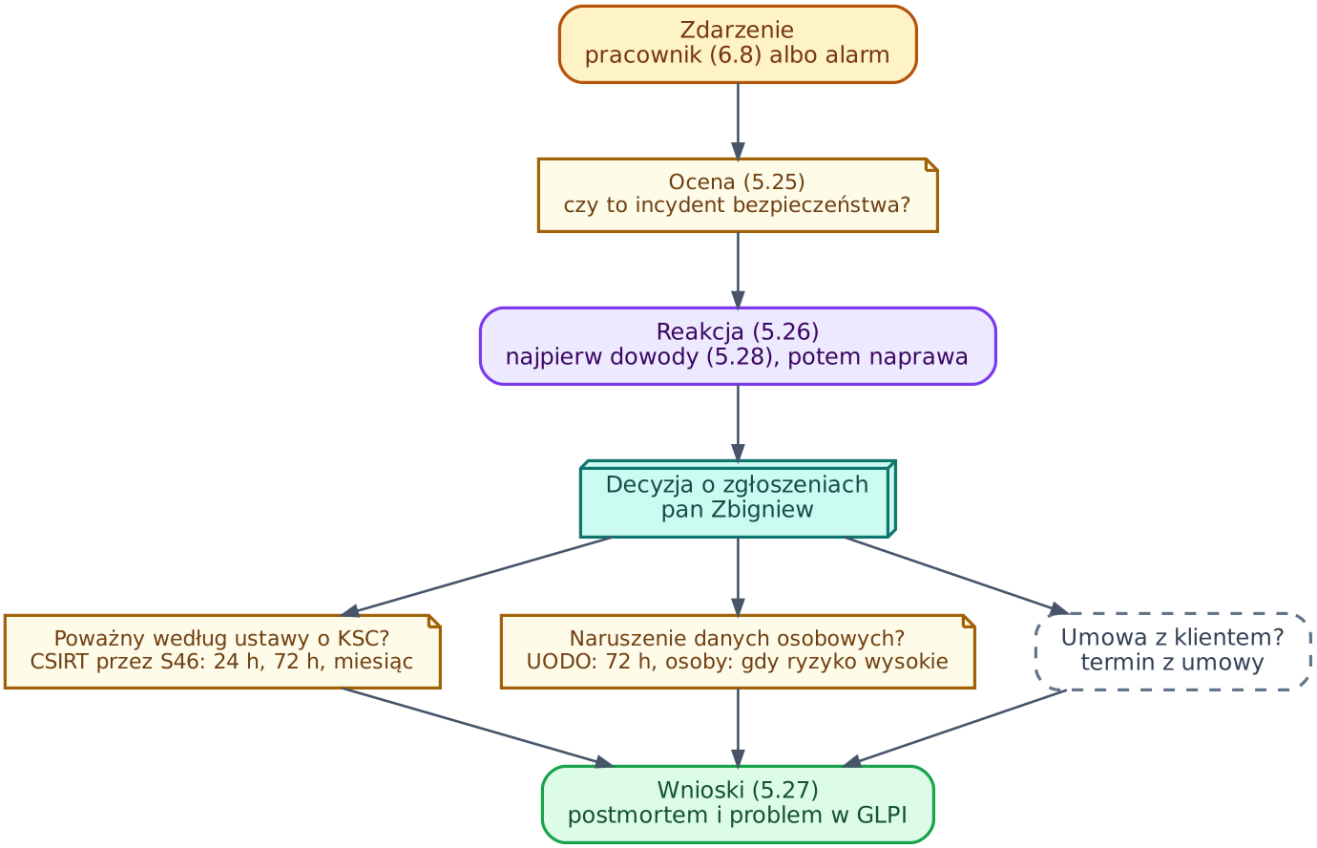
Z życia wzięte

Z ŻYCIA WZIĘTE

Czwartek, 22 października 2026, 10:00. Marek dzwoni, że dostawca WMS „wgrał w nocy poprawkę” na `ora01` i od rana raporty stanów liczą się dwa razy dłużej. W GLPI nie ma żadnej zmiany, a w umowie z dostawcą nie ma ani słowa o zapowiadaniu prac. Pan Wojtek, który akurat siedzi w pokoju IT, notuje trzy zabezpieczenia naraz: 8.32 (zmiana bez procesu), 5.20 (umowa bez wymagań bezpieczeństwa) i 5.22 (nikt nie monitoruje pracy dostawcy). Wieczorem Marek dostaje od pana Zbigniewa zadanie: aneks do umowy przed następną fakturą.

Jak to działa

Zabezpieczenia tej strony są w większości procesami, które już opisują książki o ITIL, kopiach i wysokiej dostępności. ISO/IEC 27001 dodaje do nich dwie rzeczy: perspektywę bezpieczeństwa (nie tylko „czy działa”, ale też „czy ktoś tego nie wykorzystał”) i obowiązki zewnętrzne, zwłaszcza zgłaszanie incydentów do urzędów i klientów.



Rysunek 1. Od zdarzenia do zgłoszeń: zdarzenie zgłoszone przez pracownika albo alarm, ocena, czy to incydent bezpieczeństwa, reakcja z zabezpieczeniem dowodów, a potem trzy niezależne pytania: czy incydent jest poważny w rozumieniu ustawy o KSC (CSIRT: 24 h, 72 h, miesiąc), czy doszło do naruszenia danych osobowych (UODO: 72 h) i czy umowa z klientem wymaga zgłoszenia; na końcu wnioski i postmortem (kliknięcie otwiera pełny rozmiar)

> **Pojęcie: incydent bezpieczeństwa informacji.** Zdarzenie albo seria zdarzeń, które naruszyły albo mogą naruszyć poufność, integralność lub dostępność informacji i wymagają reakcji. Każdy incydent bezpieczeństwa jest incydentem w rozumieniu ITIL, ale nie każda awaria jest incydentem bezpieczeństwa: pełny dysk logu transakcyjnego nim nie jest, zaszyfrowany udział już tak.

Zabezpieczenia po kolei

8.32 Zarządzanie zmianami

O co tu naprawdę chodzi. Zmiany w systemach i usługach przechodzą przez ustalony proces: ocena, zatwierdzenie, testy, plan wycofania, zapis [1]. Dotyczy to także zmian robionych przez dostawców.

Co audytor chce zobaczyć.

- zapisany proces z rodzajami zmian i zatwierdzającymi,
- dziennik zmian i dwie, trzy zmiany prześledzone od wniosku do zamknięcia,
- zmiany awaryjne z dokumentacją uzupełnioną po fakcie.

Jak to mamy w Zielonej. Zmiany, organ zatwierdzający i okna zmian: jak zmieniamy, żeby nic nie zepsuć z oknami, zakazem od 15 listopada do 6 stycznia i oceną ryzyka kolorem karty. Po scence dopisujemy: zmiany dostawców też mają numer w GLPI, a dostawca dostaje dostęp tylko w oknie z numerem zmiany. Dowód: fiszki „Wypisanie zmian konfiguracji” i „Wyeksportowanie dziennika zmian z GLPI”.

8.25 Bezpieczny cykl wytwarzania, 8.28 bezpieczne programowanie (nowe w 2022) i 8.31 rozdzielenie środowisk

O co tu naprawdę chodzi. Oprogramowanie, które piszemy, powstaje według zasad bezpieczeństwa od pomysłu do wdrożenia: przegląd kodu, testy, brak sekretów w kodzie, znane biblioteki, osobne środowiska rozwojowe, testowe i produkcyjne [1][2]. 8.28 jest nowe i dotyczy samego pisania kodu: znane błędy, zależności, przegląd.

Co audytor chce zobaczyć.

- opis, jak zespół Oli wytwarza i wdraża aplikacje (gałęzie, przegląd, budowanie, wdrożenie),
- ochronę gałęzi i przegląd kodu w praktyce,
- rozdzielenie środowisk i brak prawdziwych danych osobowych w testach (powiązanie z 8.11).

Jak to mamy w Zielonej. Gitea z Actions (Gitea Actions: runner i pierwszy workflow), TeamCity (Pierwszy projekt: cennik z Gitea budowany w TeamCity), sekrety poza repozytorium i Asystenci kodujący i agenci w terminalu: jak pracować bezpiecznie dla kodu pisanego z AI. Laboratorium `k3s01` oddziela próby od produkcji. Zapisanych zasad bezpiecznego programowania zespołu Oli jeszcze nie ma: to zadanie dla Oli w planie postępowania. Dowód: fiszki „Sprawdzenie ochrony gałęzi głównej” i „Skanowanie historii repozytorium”.

5.19 do 5.22 Dostawcy: od wyboru do monitorowania

O co tu naprawdę chodzi. Wiemy, którzy dostawcy mają dostęp do naszych informacji albo od których zależą nasze usługi, wymagania bezpieczeństwa są w umowach, łańcuch dostaw ICT (Information and Communication Technology, czyli sprzęt, oprogramowanie i usługi informatyczne) jest brany pod uwagę, a pracę dostawców monitorujemy i oceniamy [1].

Co audytor chce zobaczyć.

- rejestr dostawców z krytycznością,
- przykładową umowę z wymaganiami bezpieczeństwa (poufność, zgłaszanie incydentów, dostęp zdalny, prawo do audytu),
- ocenę kluczowego dostawcy z ostatniego roku.

Jak to mamy w Zielonej. Dostawcy krytyczni: dostawca WMS, dostawca Optimy, operator łącza, Microsoft (Microsoft 365, Azure), AWS (archiwum), Fortinet (FortiGuard). Rejestr w GLPI (fiszka), umowy powierzenia danych przy RODO, zasady dostępu zdalnego jak w ryzyku R-06. Luka ze scenki (umowa WMS bez wymagań) jest w planie postępowania. Ustawa o KSC też każe brać pod uwagę ryzyko łańcucha dostaw, więc rejestr dostawców przyda się dwa razy. Dowód: fiszka „Przegląd rejestru dostawców i umów”.

5.23 Bezpieczeństwo korzystania z usług chmurowych (nowe w 2022)

O co tu naprawdę chodzi. Zanim zaczniemy korzystać z usługi w chmurze, ustalamy, kto za co odpowiada, jak ją zabezpieczamy po naszej stronie, jak ją monitorujemy i jak z niej wyjdziemy [1][2]. Chmura nie zdejmuje z nas odpowiedzialności za konfigurację, konta i dane.

Co audytor chce zobaczyć.

- listę usług chmurowych z właścicielem i oceną,
- podział odpowiedzialności z dostawcą (model współdzielonej odpowiedzialności),
- konfigurację bezpieczeństwa po naszej stronie (MFA, dostęp warunkowy, niezmienność kopii) i plan wyjścia.

Jak to mamy w Zielonej. Microsoft 365 i Entra ID (książka o Intune), Azure i AWS jako zimne archiwum (Zimne archiwum w chmurze: Azure Blob Storage i Amazon S3 Glacier), `edge-az01` w Azure, pojęcia na stronie Chmura: pojęcia, które trzeba znać zanim cokolwiek uruchomimy. Rejestr usług chmurowych to sekcja rejestru dostawców. Dowód: fiszka „Przegląd aplikacji chmurowych z logowaniem przez Entra ID”.

5.7 Informacje o zagrożeniach (nowe w 2022)

O co tu naprawdę chodzi. Zbieramy i analizujemy informacje o zagrożeniach, które dotyczą naszej firmy, i na ich podstawie zmieniamy zabezpieczenia albo ocenę ryzyka [1][2]. W małej firmie to nie jest zespół analityków, tylko kilka dobrze wybranych źródeł i nawyk, że ktoś je czyta.

Co audytor chce zobaczyć.

- listę źródeł (CERT Polska, biuletyny producentów, wykaz KEV),
- dowód, że informacja doprowadziła do działania (zgłoszenie, zmiana awaryjna, nowe ryzyko),
- kto i jak często przegląda źródła.

Jak to mamy w Zielonej. Źródła: ostrzeżenia CERT Polska, biuletyny bezpieczeństwa Fortinet i Microsoftu (Patch Tuesday), wykaz KEV agencji CISA, alerty Defendera o podatnościach. Przegląd raz w tygodniu przy przeglądzie wtorkowym, a krytyczna informacja o naszym sprzęcie od razu jako zgłoszenie. Przykład decyzji: ćwiczenie 3 na stronie o zmianach (krytyczna luka w zaporze i zmiana awaryjna). Dowód: fiszka „Wyszukanie nowych wykorzystywanych podatności” i zgłoszenia z kategorii informacji o zagrożeniach.

5.24 do 5.28 i 6.8 Incydenty: od zgłoszenia do wniosków

O co tu naprawdę chodzi. Mamy przygotowany sposób reagowania na incydenty (role, procedury, kontakty), oceniamy zdarzenia, reagujemy według procedury, uczymy się z incydentów i zabezpieczamy dowody tak, żeby nadawały się do dalszego użycia [1]. Pracownicy wiedzą, jak i gdzie zgłosić podejrzane zdarzenie (6.8).

Co audytor chce zobaczyć.

- procedurę z rolami i kontaktami (także do CSIRT, UODO, policji, ubezpieczyciela),
- przykład incydentu bezpieczeństwa z oceną, przebiegiem, czasem i wnioskami,
- sposób zabezpieczania dowodów i dowód, że pracownicy wiedzą, jak zgłaszać.

Jak to mamy w Zielonej. Incydent i incydent poważny: od zgłoszenia do zamknięcia z rolami i obowiązkami prawnymi, Alerty, incydenty i EDR: co robimy, gdy Defender coś znajdzie, Problemy, analiza przyczyn i postmortem: żeby ta sama awaria nie wróciła dla wniosków. Terminy z ustawy o KSC i RODO zbiera strona o przepisach. Brakuje listy kontaktów zewnętrznych w jednym miejscu: dopisujemy ją do procedury (właściwy CSIRT, UODO, policja, ubezpieczyciel, jeśli jest polisa,

kontakt bezpieczeństwa w sieci sklepów). Dowód: fiszki „Policzenie sumy kontrolnej” i „Zestawienie incydentów bezpieczeństwa”.

8.13 Kopie zapasowe

O co tu naprawdę chodzi. Kopie informacji, oprogramowania i systemów powstają według uzgodnionych zasad i są regularnie sprawdzane przez odtworzenie [1].

Co audytor chce zobaczyć.

- zasady: co kopiujemy, jak często, jak długo trzymamy, gdzie,
- protokoły testów odtworzenia z kilku kwartałów z czasami,
- ochronę kopii przed skasowaniem i zaszyfrowaniem.

Jak to mamy w Zielonej. Cała książka o kopiach: Strategia kopii zapasowych Zielonej: RPO, RTO, reguła 3-2-1-1-0 i dwie lokalizacje, Serwery kopii bkp01 i bkp02: restic, kopia krzyżowa i niezmienność i Testy odtwarzania: plik, maszyna, baza i cała lokalizacja z kalendarzem testów (10.11.2026, 2.02, 4.05, 3.08 i 5.10.2027). To zabezpieczenie Zielona ma najlepiej udokumentowane. Dowód: fiszki o restic i protokoły testów.

8.14 Nadmiarowość środków przetwarzania informacji

O co tu naprawdę chodzi. Systemy, od których zależy firma, mają zapas wystarczający do wymagań dostępności: drugi serwer, drugie łącze, drugi zasilacz [1].

Co audytor chce zobaczyć.

- wymagania dostępności dla usług (RTO, RPO) i to, jak nadmiarowość je spełnia,
- listę pojedynczych punktów awarii z decyzjami,
- testy przełączenia.

Jak to mamy w Zielonej. Macierz wysokiej dostępności usług Zielonej: poziom rezerwy każdej usługi, zależności i kolejność prac z 16 pojedynczymi punktami awarii, etapami prac i kalendarzem testów przełączenia (9.02, 9.03, 11.05, 10.08 i 12.10.2027). Ryzyka z niej, na które pan Zbigniew nie dał budżetu (druga zapora, drugi UPS), wpisujemy do rejestru jako zaakceptowane. Dowód: macierz i protokoły testów przełączenia.

5.29 Bezpieczeństwo w czasie zakłóceń i 5.30 gotowość ICT do ciągłości działania (nowe w 2022)

O co tu naprawdę chodzi. Gdy firma działa w trybie awaryjnym, bezpieczeństwo informacji nie znika (5.29), a infrastruktura IT jest przygotowana, zaplanowana i przetestowana tak, żeby spełnić cele ciągłości działania firmy (5.30) [1][2]. 5.30 jest nowe i przenosi uwagę z „mamy kopie” na „wiemy, w jakiej kolejności i w jakim czasie wstaniemy”.

Co audytor chce zobaczyć.

- analizę wpływu na działalność albo przynajmniej uzgodnione RTO i RPO usług z ich właścicielami,
- plan odtworzenia z kolejnością usług,
- test planu i wnioski z niego, w tym to, czy zabezpieczenia (na przykład logowanie, kontrola dostępu) działały w trybie awaryjnym.

Jak to mamy w Zielonej. RTO i RPO w macierzy wysokiej dostępności, kolejność odtwarzania usług po utracie serwerowni na stronie o testach odtwarzania, test całej lokalizacji w październiku. Brakuje jednej strony „Plan ciągłości działania IT Zielonej”, która zbiera te elementy, kontakty i decyzje biznesowe (praca ręczna w magazynie, wstrzymanie wysyłek). To dokument do napisania w pierwszym kwartale 2027, z panem Zbigniewem i Markiem.

7.4 Monitorowanie bezpieczeństwa fizycznego (nowe w 2022) i 7.14 bezpieczne pozbycie się sprzętu

O co tu naprawdę chodzi. Pomieszczenia z informacjami i sprzętem są stale obserwowane (kamery, alarm, kontrola wejść) pod kątem nieuprawnionego wejścia (7.4), a sprzęt z nośnikami przed oddaniem, sprzedażą albo zezłomowaniem jest sprawdzony i wyczyszczony (7.14) [1][2]. To zabezpieczenia fizyczne, ale w małej firmie robi je IT.

Co audytor chce zobaczyć.

- system monitorowania serwerowni z zapisem i przeglądem zdarzeń,
- rejestr wejść do serwerowni i przegląd uprawnień kart,
- protokoły kasowania albo zniszczenia nośników ze sprzętu wycofanego w ostatnim roku.

Jak to mamy w Zielonej. Monitoring wizyjny: kamery IP, ONVIF, rejestrator i RODO, Kontrola dostępu: karty, PIN, biometria, kontrolery i audyt uprawnień, Alarm i ochrona: centrala, czujki, strefy i połączenie z agencją, Audyt fizyczny serwerowni i biura: lista kontrolna i własny czytnik kart i niszczenie nośników ze strony o 8.10. Dowód: raport z kontroli dostępu, protokoły niszczenia.

Częste błędy

Objaw	Przyczyna	Co robimy
Dostawca zmienia system bez wiedzy IT	brak wymagań w umowie, stały dostęp zdalny	aneks z wymaganiami, dostęp tylko w oknie z numerem zmiany
Lista dostawców obejmuje tylko tych, którym płacimy fakturą	pominięte usługi bezpłatne i dodane przez pracowników	przegląd aplikacji w Entra ID i ruchu na `fw01` raz w roku
Incydent bezpieczeństwa zamknięty jak zwykła awaria	brak kategorii i oceny	kategoria „Incydent bezpieczeństwa”, ocena terminów zgłoszeń przy rejestracji
Dowody z incydentu zebrane po restarcie	pośpiech przy przywracaniu	najpierw logi, lista procesów, obraz, suma kontrolna, potem naprawa
Kopie testowane, plan ciągłości nie	myślenie „kopia to ciągłość”	plan z kolejnością usług i decyzjami biznesowymi, test całej lokalizacji raz w roku
Kod trafia do produkcji bez przeglądu	ochrona gałęzi wyłączona „na chwilę”	ochrona na stałe, wyjątek tylko przez zmianę awaryjną
Informacje o zagrożeniach czytane, bez śladu decyzji	brak zapisu	każda informacja dotycząca naszego sprzętu to zgłoszenie z decyzją

□□ Ćwiczenia

1. Sobota, 7:20. Graylog alarmuje o masowej zmianie nazw plików na `fs01`. Które terminy zewnętrzne mogą zacząć biec i od czego zależą?

Odpowiedź

Jeśli Zielona jest podmiotem ważnym i incydent okaże się poważny w rozumieniu ustawy o KSC, biegnie 24 godziny na wczesne ostrzeżenie do właściwego CSIRT od wykrycia, potem 72 godziny na zgłoszenie i miesiąc na sprawozdanie końcowe. Jeśli na udziałach były dane osobowe i doszło do ich naruszenia, biegnie 72 godziny na zgłoszenie do UODO od stwierdzenia naruszenia. Jeśli umowa z siecią sklepów wymaga zgłoszenia, biegnie termin z umowy. O

zgłoszeniach decyduje zarząd, my zbieramy fakty z godzinami.

1. Ola chce wyłączyć ochronę gałęzi w repozytorium cennika na czas pilnej poprawki przed świętami. Co mówią 8.25, 8.32 i kalendarz Zielonej?

Odpowiedź

Przed świętami trwa zakaz zmian (15 listopada do 6 stycznia), więc wdrożenie na produkcję to zmiana awaryjna albo zmiana za zgodą pana Zbigniewa. Ochrony gałęzi nie wyłączamy: poprawka idzie przez pull request z szybkim przeglądem drugiej osoby, a wdrożenie przez zmianę awaryjną z wpisem w GLPI uzupełnionym następnego dnia.

1. Audytor pyta, skąd wiemy, że dostawca WMS ma odpowiednie zabezpieczenia. Co odpowiadamy po scence z tej strony?

Odpowiedź

Uczciwie: do tej pory nie mieliśmy tego w umowie. Pokazujemy wpis R-06 w rejestrze ryzyk, zadanie w planie postępowania (aneks z wymaganiami bezpieczeństwa, zgłaszaniem incydentów i zasadami dostępu zdalnego), tymczasowe zabezpieczenia (konto na czas pracy, VPN z MFA) i termin. To prawdopodobnie da niezgodność małą, a nie dużą, bo luka jest znana i zarządzana.

1. Dlaczego 5.30 nie jest spełnione samymi testami odtwarzania z kalendarza kopii?

Odpowiedź

Bo testy odtwarzania sprawdzają, czy dane da się odzyskać, a 5.30 wymaga gotowości całej infrastruktury IT do celów ciągłości firmy: kolejności usług, czasów zgodnych z RTO uzgodnionymi z właścicielami, ludzi, kontaktów i decyzji biznesowych. Testy są dowodem częściowym; brakuje planu ciągłości działania IT i testu, który sprawdza cały plan.

Powiązane: Zabezpieczenia dla IT po ludzku: dostęp, tożsamość i konta uprzywilejowane · Zabezpieczenia dla IT po ludzku: systemy, sieć i dane · ISO/IEC 27001 a przepisy: NIS2 i ustawa o KSC, RODO, DORA i inne · Kopie hostów Dockera narzędziami do kopii: Veeam i odpowiedniki · Bezpieczeństwo AI w infrastrukturze: modele, agenci i MCP w sieci firmy

Źródła: [1] Parafraza własna sensu zabezpieczeń 5.7, 5.19 do 5.30, 6.8, 7.4, 7.14, 8.13, 8.14, 8.25, 8.28, 8.31 i 8.32 na podstawie publicznych opracowań: hightable.io, „ISO 27001 Annex A controls reference guide”; isms.online, opisy zabezpieczeń Załącznika A 2022; advisera.com, baza wiedzy

ISO 27001. · [2] Lista nowych zabezpieczeń 2022: hightable.io i isms.online. · Terminy zgłaszania incydentów: ustawa z 23 stycznia 2026 o zmianie ustawy o krajowym systemie cyberbezpieczeństwa, Dz.U. 2026 poz. 252, art. 11 ust. 1 w nowym brzmieniu (tekst z api.sejm.gov.pl); RODO art. 33. · Wykaz KEV: cisa.gov, Known Exploited Vulnerabilities Catalog, plik JSON pod adresem z Fiszki (pola `vendorProject`, `product`, `cveID`, `dateAdded`). · Polecenia: restic.readthedocs.io (snapshots, check); Microsoft Learn (wbadmin get versions); gitleaks (opis na stronie o asystentach kodujących); git-log(1). · Ścieżki GLPI i Entra: menu do sprawdzenia w naszych wersjach. · Numer CVE w przykładzie zastąpiony znakami `x`.