Smarter technology for all

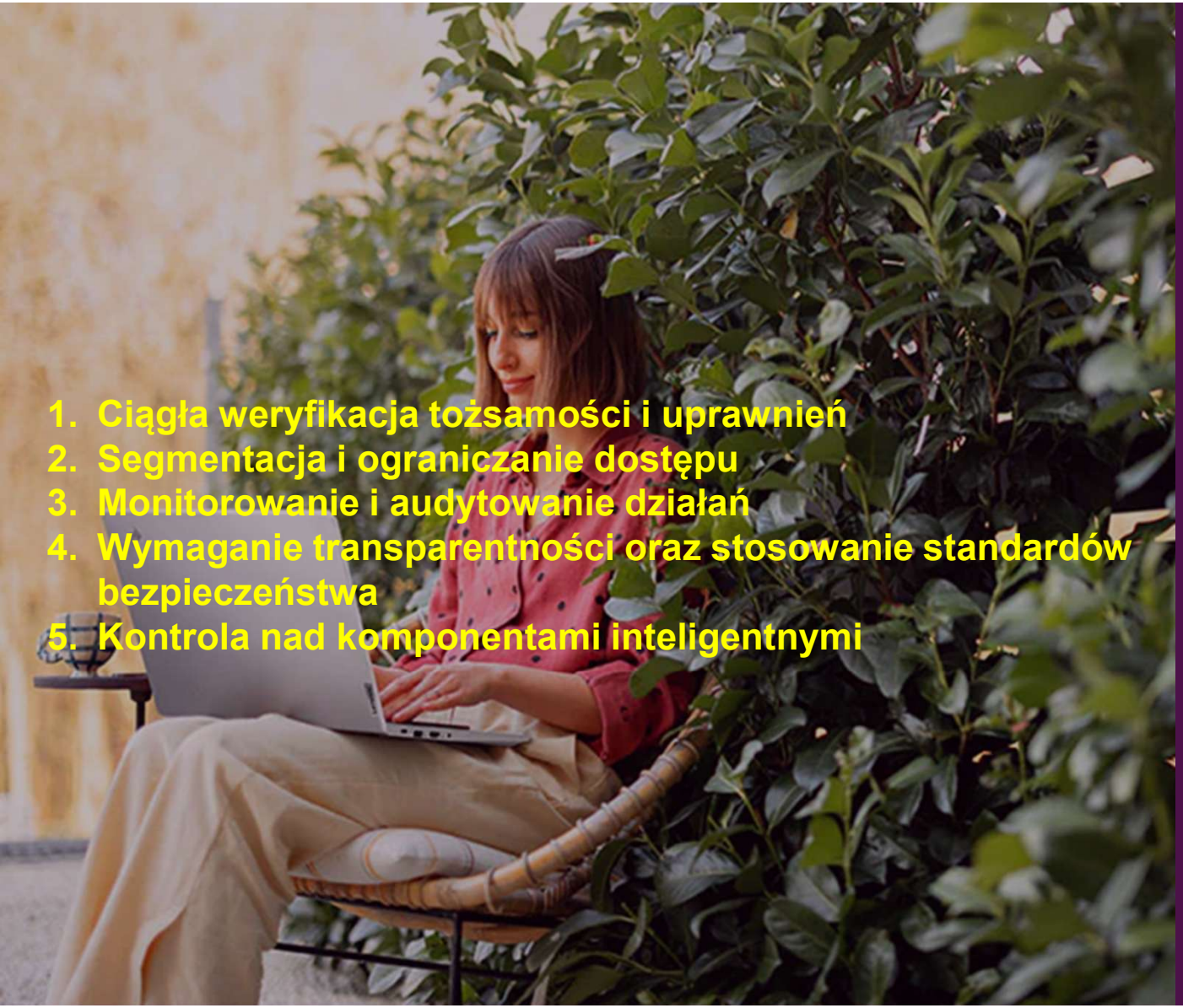
Niewidzialny fundament ZERO TRUST: bezpieczeństwo urządzeń z perspektywy zarządu

16 czerwca 2026

2026 Lenovo

Zero Trust

wobec urządzeń to podejście, w którym każde urządzenie musi być zweryfikowane, zgodne z polityką bezpieczeństwa i objęte minimalnym zakresem dostępu, niezależnie od tego, skąd łączy się z zasobami



1. Ciągła weryfikacja tożsamości i uprawnień
2. Segmentacja i ograniczanie dostępu
3. Monitorowanie i audytowanie działań
4. Wymaganie transparentności oraz stosowanie standardów bezpieczeństwa
5. Kontrola nad komponentami inteligentnymi

ZERO TRUST W PRAKTYCE

Brak domyślnego zaufania wobec jakiegokolwiek elementu procesu zakupowego czy produkcyjnego

CZY ATAKI NA ŁAŃCUCH DOSTAW TO CZYSTE SiFi?

2020

- **SolarWinds Orion**

2021

- **Kaseya VSA**
- **Codecov**
- **Log4j**

2023

- **3CX**

Jak to wygląda w świetle polskiego prawa - 1

1. Odpowiedzialność cywilna (odszkodowawcza) wobec spółki.

Członkowie zarządu są odpowiedzialni wobec spółki za szkody wyrządzone działaniem lub zaniechaniem, jeśli zachodzi ich „wina” i :naruszenie obowiązków” (art. 483 k.s.h. dla spółek akcyjnych oraz art. 293 k.s.h. dla spółek z o.o.)

W praktyce w przypadku ataków na łańcuch dostaw:

- Jeśli zarząd nie wdrożył stosownych środków cyberbezpieczeństwa, zaniedbał audyty, nie wypracował właściwych polityk zabezpieczających, zignorował znane ryzyka wówczas działania takie mogą zostać uznane za: NIENALEŻYTE ZARZĄDZANIE i dalej dają podstawę do POWÓDZTWA O NAPRAWIENIE SZKODY



Jak to wygląda w świetle polskiego prawa - 2

2. Odpowiedzialność pracownicza

Jeśli członek zarządu jest zatrudniony na umowę o pracę to ponosi odpowiedzialność pracowniczą za szkodę wyrządzoną pracodawcy.
W przypadku cyberataku i braku należytej staranności:

- Rozwiązanie umowy o pracę (w tym bez wypowiedzenia z winy pracownika
- Dochodzenie odszkodowania na zasadach Kodeksu Pracy

3. Odpowiedzialność karna i skarbowa

W skrajnych przypadkach, gdy zarząd wyrządzi spółce znaczącą szkodę majątkową lub dopuści się przestępstw – niezgłoszenie upadłości, ukrywanie faktów itp. Może dojść do odpowiedzialności karnej lub karno-skarbowej. W praktyce:

-kary grzywny
-ograniczenia wolności
-zakaz prowadzenia działalności gospodarczej lub pełnienia funkcji w zarządzie



Lenovo 2026 Lenovo

Jak to wygląda w świetle polskiego prawa - 3

4. Odpowiedzialność za długi spółki (Art. 299 k.s.h)

W przypadku niewypłacalności spółki, członkowie zarządu mogą być osobiście odpowiedzialni za długi spółki z majątku prywatnego, jeśli:

- nie złożyli wniosku o ogłoszenie upadłości lub restrukturyzację w terminie
- nie wykazali, że nie ponoszą winy w braku zapłaty
- nie wykazali realnego majątku spółki do egzekucji

Cyberatak, który prowadzi do przestoju, strat, utraty płynności i niewypłacalności, może wiec bezpośrednio uruchomić tę odpowiedzialność

5. Odpowiedzialność za podatki i ZUS

Członkowie zarządu odpowiadają solidarnie za zaległości podatkowe o składki ZUS powstałe w czasie pełnienia swoich funkcji (art. 116 ordynacji podatkowej)
Cyberatak i przestój w produkcji mogą prowadzić do:
-braku uregulowania zobowiązań podatkowych
-zaległości ZUS
W przypadku braku wypłacalności organy mogą ściągać te kwoty od zarządu z majątku prywatnego



Lenovo 2026 Lenovo

Jak to wygląda w świetle polskiego prawa - 4

6. RODO i nadzór danych

W sytuacji w której atak na łańcuch dostaw powoduje naruszenie danych osobowych zarząd odpowiada za:

- Powiadomienie organu UODO w ciągu 72 godzin
- Powiadomienie osób, których dane dotyczą,
- Wdrożenie środków naprawczych

Brak tych działań może prowadzić do kar pieniężnych i odpowiedzialności odszkodowawczej wobec osób poszkodowanych



KONKRETNE DZIAŁANIA

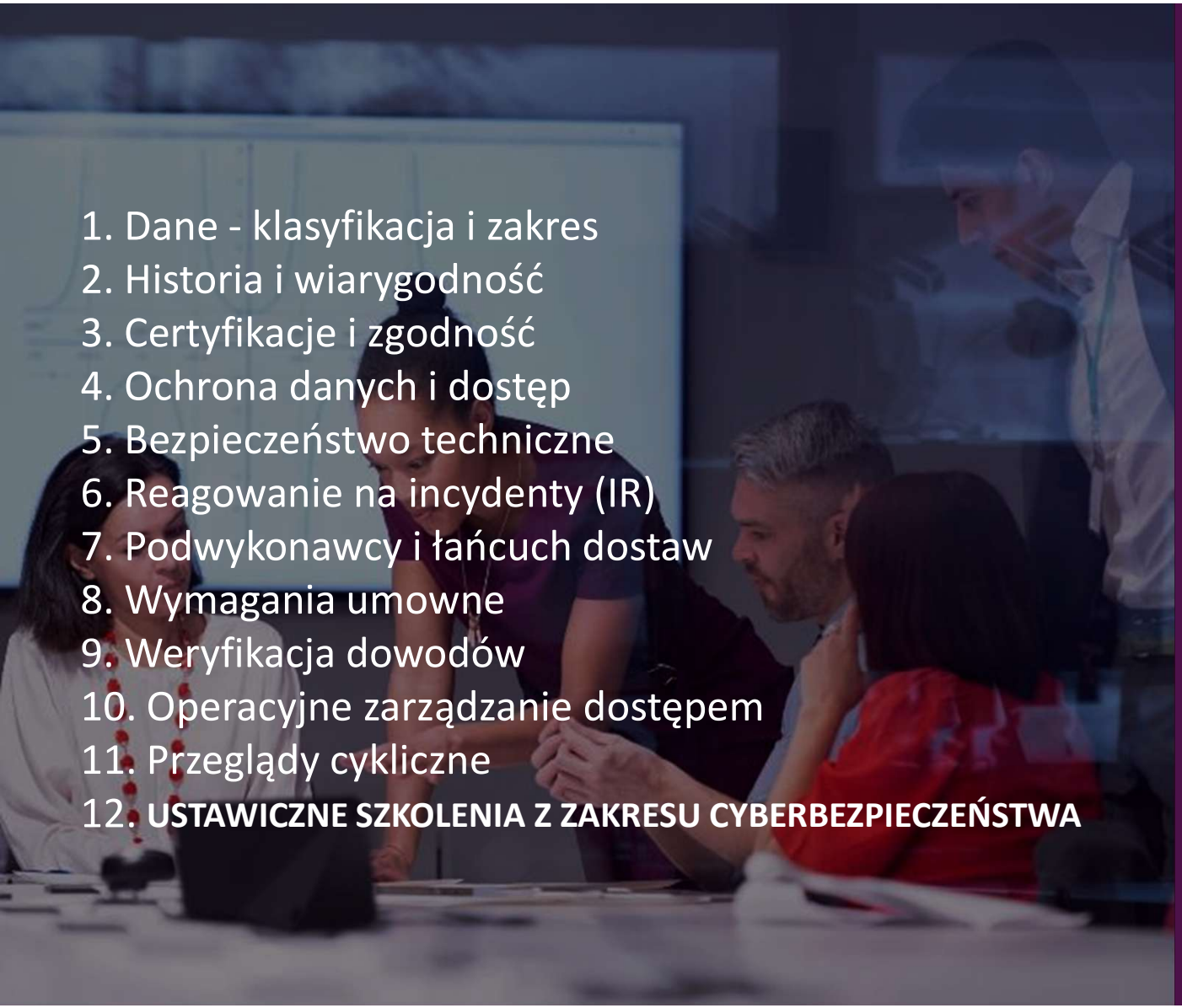
Jakie kroki audytowe pozwolą zarządowi ograniczyć ryzyko prawne

Audyt prawny i ryzyka korporacyjnego	• Przegląd dokumentacji prawnej • Wywiady i konsultacje w celu zidentyfikowania zagrożeń	• Ocena ryzyka • Strategia zarządzania ryzykiem
Audyt cyberbezpieczenstwa I bezpieczeństwa IT	• Audyt bezpieczeństwa infrastruktury i sieci • Audyt bezpieczeństwa łańcucha dostaw • Testy penetracyjne • Audyt poufności i integralności danych	• Weryfikacja zgodności z normami ISO27001, dyrektywą NIS2 oraz zgodności z KSC
Audyt RODO i ochrony danych osobowych	• Analiza ryzyka zgodnie z RODO • Przegląd dokumentacji RODO • Weryfikacja procedur powiadamiania	
Audyt ciągłości działania I planów awaryjnych	• Audyt dokumentacji ciągłości procesów biznesowych • Testy planów awaryjnych • Określenie maksymalnego czasu przestoju oraz utraty danych dla systemów krytycznych	
Audyt zgodności z regulacjami i wymaganiami sektorowymi	• Zgodność z NIS2 (dla podmiotów kluczowych lub istotnych • Zgodność z wymaganiami sektorowymi (energetyka, transport, finanse ochrona	zdrowia) • Przegląd zobowiązań kontraktowych z klientami i partnerami/dostawcami
Audyt procesów decyzyjnych i dokumentacji zarządu	• Przegląd protokołów z posiedzeń zarządu po kątem regularności omawiania kwestii z zakresu cyberbezpieczeństwa	• Dokumentacja decyzji strategicznych (budżety na bezpieczeństwo, inwestycje w ochronę i audyty • Weryfikacja procedur eskalacji
Audyt umów z dostawcami i zarządzanie ryzykiem łańcucha dostaw	• Przegląd umów z kluczowymi dostawcami, klauzule bezpieczeństwa, SLA prawo do audytu, obowiązek raportowania incydentów • Audyt bezpieczeństwa dostawców,	ocena ich polityk bezpieczeństwa, certyfikatów, wyników testów • Mapowanie zależności (identyfikacja dostawców drugiego i trzeciego poziomu
Audyt ubezpieczeniowy i transfer ryzyka	• Przegląd polis ubezpieczeniowych: cyber ubezpieczenie, ubezpieczenie odpowiedzialności cywilnej zarządu, ubezpieczenie majątku i przestoju	• Weryfikacja zakresu ochrony np. czy polisa obejmuje ataki na łańcuch dostaw, koszty incydentu, odszkodowania, grzywny



ILE MOŻE KOSZTOWAĆ INCYDENT

JLR



1. Dane - klasyfikacja i zakres
2. Historia i wiarygodność
3. Certyfikacje i zgodność
4. Ochrona danych i dostęp
5. Bezpieczeństwo techniczne
6. Reagowanie na incydenty (IR)
7. Podwykonawcy i łańcuch dostaw
8. Wymagania umowne
9. Weryfikacja dowodów
10. Operacyjne zarządzanie dostępem
11. Przeglądy cykliczne
12. **USTAWICZNE SZKOLENIA Z ZAKRESU CYBERBEZPIECZEŃSTWA**

I NA KONIEC

Co warto wziąć pod uwagę i rozważyć wdrożenie we własnej firmie