cyllium

LEAD YOUR BUSINESS PROTECTED

BEZPEČNOSTNÉ OPATRENIA V NIS2

aktuálny stav

11. 6. 2024
Marián ILLOVSKÝ

Marián Illovský

Spoluzakladateľ a auditný partner Cyllium group

Certified Information system Auditor (CISA),
Certified Internal Auditor (CIA),
Certified Data Privacy Solutions Engineer (CDPSE),
Certified Information Security Manager (CISM),
Global Industrial Cyber Security Professional (GICSP),
Certifikovaný audítor a manažér kybernetickej bezpečnosti

- viac ako 20-ročné skúsenosti s auditom informačnej bezpečnosti a manažmentom kybernetickej bezpečnosti,
- externý posudzovateľ pre Slovenskú národnú akreditačnú službu pre ISO 27001, ISO 20000-1, ISO 22301, eIDAS a pre certifikáciu audítorov a manažérov kybernetickej bezpečnosti.
- externý posudzovateľ pre eIDAS pre Slovinskú akreditáciu

LEAD
YOUR
BUSINESS
PROTECTED

Skupina Cyllium

- poskytuje komplexné služby v oblasti informačnej a kybernetickej bezpečnosti na Slovensku i v zahraničí

- vykonáva auditné, expertné a technologické služby pod dohľadom skúsených profesionálov s medzinárodnými skúsenosťami a certifikáciami

Členmi skupiny sú spoločnosti:

- auditori.it, s. r. o.
- Cyllium SK, s. r. o.
- Cyllium IT, s. r. o.

LEAD
YOUR
BUSINESS
PROTECTED

O nás

Certified Internal Auditor

Certified Data Privacy Solutions Engineer

Certified Information Systems Auditor

Certified Information Security Manager

PRINCE2 Foundation

ISA/IEC 62443 Cybersecurity Fundamentals Specialist

ISA/IEC 62443 Cybersecurity Risk Assessment Specialist

ISA/IEC 62443 Cybersecurity Design Specialist

ISA/IEC 62443 Cybersecurity Maintenance Specialist

ISA/IEC 62443 Cybersecurity Expert

Certified Information Systems Security Professional

Microsoft Certified System Engineer

Certified Ethical Hacker

The Global Industrial Cyber Security Professional

LEAD
YOUR
BUSINESS
PROTECTED

O nás


Centrálny depozitár cenných papierov SR


DFNKE
DETSKÁ FAKULTNÁ
NEMOCNICA KOŠICE


GGE


BURZA CENNÝCH PAPIEROV V BRATISLAVE


DIGI
SLOVAKIA


AGEL SK


MINISTERSTVO
ZDRAVOTNÍCTVA
SLOVENSKEJ REPUBLIKY


NÁRODNÝ
INŠPEKTORÁT
PRÁCE


ÚGKK SR


MARTIN


MINISTERSTVO
ZAHRANIČNÝCH VECÍ
A EURÓPSKYCH ZÁLEŽITOSTÍ
SLOVENSKEJ REPUBLIKY


seps
Slovenská
elektrizačná
prenosová
sústava


NÁRODNÉ LESNÍCKE CENTRUM
NATIONAL FOREST CENTRE


SLOVENSKÁ
BANKOVÁ
ASOCIÁCIA


MINISTERSTVO
FINANCIÍ
SLOVENSKEJ REPUBLIKY


SPRÁVA ŠTÁTNYCH
HMOTNÝCH REZERV
SLOVENSKEJ REPUBLIKY


STUPAVA


NAJVYŠŠÍ SÚD
SLOVENSKEJ REPUBLIKY


SLOVENSKÁ ZÁRUČNÁ
A ROZVOJOVÁ BANKA


tasr


NAJVYŠŠÍ
SPRÁVNY SÚD
SLOVENSKEJ REPUBLIKY


ŠTÁTNY VETERINÁRNY
A POTRAVINOVÝ ÚSTAV


Webglob


websupport


LEAD
YOUR
BUSINESS
PROTECTED

O čom budeme diskutovať?

01 Bezpečnostné opatrenia v NIS2

- zmeny oproti NIS(1)
- porovnanie s aktuálnym stavom

02 Audit KB

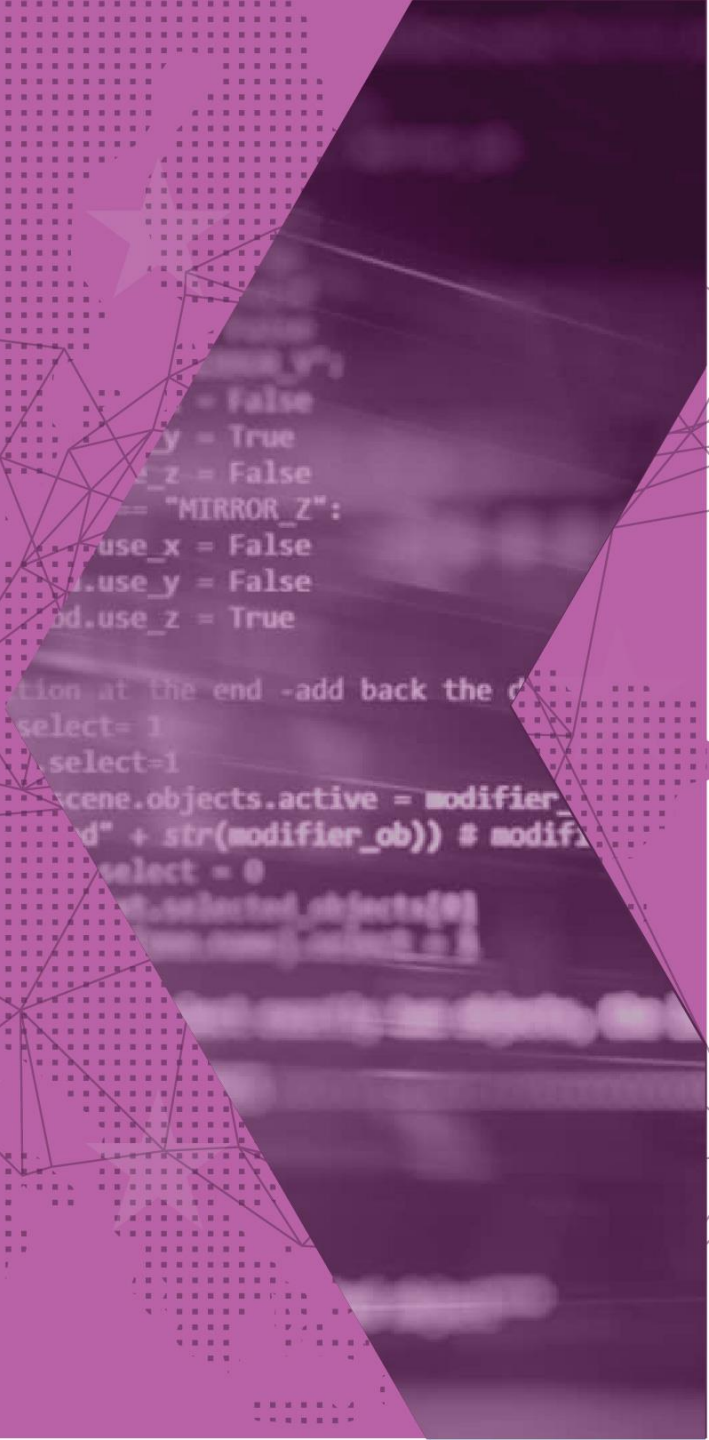
- bude / nebude?

03 Čo ďalej?

- očakávané aktivity
- následné činnosti

LEAD YOUR BUSINESS PROTECTED

01/ Bezpečnostné opatrenia v NIS2



Článok 20 - Riadenie

- Členské štáty zabezpečia, aby **riadiace orgány kľúčových a dôležitých subjektov schválili opatrenia na riadenie kybernetických rizík**, ktoré tieto subjekty prijali s cieľom dosiahnuť súlad s článkom 21, **dohliadali na jeho vykonávanie a aby mohli byť brané na zodpovednosť, ak subjekty porušujú** uvedený článok.

- Členské štáty zabezpečia, aby **členovia riadiacich orgánov** kľúčových a dôležitých subjektov **boli povinní absolvovať odbornú prípravu**, a kľúčové a dôležité subjekty podporia v tom, **aby svojim zamestnancom pravidelne poskytovali podobnú odbornú prípravu** a ich zamestnanci tak získali dostatočné znalosti a zručnosti a vedeli rozpoznať riziká a posúdiť postupy riadenia kybernetických rizík a ich vplyv na služby poskytované subjektom.

LEAD
YOUR
BUSINESS
PROTECTED

Článok 21 - Opatrenia na riadenie kybernetických rizík 1

- zásady analýzy rizík a bezpečnosti informačných systémov;
- riešenie incidentov;
- kontinuitu činností, ako je riadenie zálohovania a obnova systému po havárii, a krízové riadenie;
- bezpečnosť dodávateľského reťazca vrátane bezpečnostných aspektov týkajúcich sa vzťahov medzi jednotlivými subjektmi a ich priamymi dodávateľmi alebo poskytovateľmi služieb;
- bezpečnosť pri nadobúdaní, vývoji a údržbe siete a informačných systémov vrátane riešenia zraniteľností a zverejňovania informácií o zraniteľnostiach;

LEAD YOUR BUSINESS PROTECTED

Článok 21 - Opatrenia na riadenie kybernetických rizík 2

- zásady a postupy posudzovania účinnosti opatrení na riadenie kybernetických rizík;
- základné postupy kybernetickej hygieny a odborná príprava v oblasti kybernetickej bezpečnosti;
- zásady a postupy používania kryptografie, prípadne šifrovania;
- bezpečnosť ľudských zdrojov, zásady kontroly prístupu a správu aktív;
- v prípade potreby používanie riešení viacstupňovej alebo kontinuálnej autentifikácie, zabezpečenej hlasovej, obrazovej a textovej komunikácie a zabezpečených systémov komunikácie v núdzových situáciách v rámci subjektu.

LEAD YOUR BUSINESS PROTECTED

Článok 21 - Opatrenia na riadenie kybernetických rizík 1 vs V362

- zásady analýzy rizík a bezpečnosti informačných systémov; **§6**
- riešenie incidentov; **§17**
- kontinuitu činností, ako je riadenie zálohovania a obnova systému po havárii, a krízové riadenie; **§17b**
- bezpečnosť dodávateľského reťazca vrátane bezpečnostných aspektov týkajúcich sa vzťahov medzi jednotlivými subjektmi a ich priamymi dodávateľmi alebo poskytovateľmi služieb; **§9**
- bezpečnosť pri nadobúdaní, vývoji a údržbe siete a informačných systémov vrátane riešenia zraniteľností a zverejňovania informácií o zraniteľnostiach; **§14, §11**

LEAD YOUR BUSINESS PROTECTED

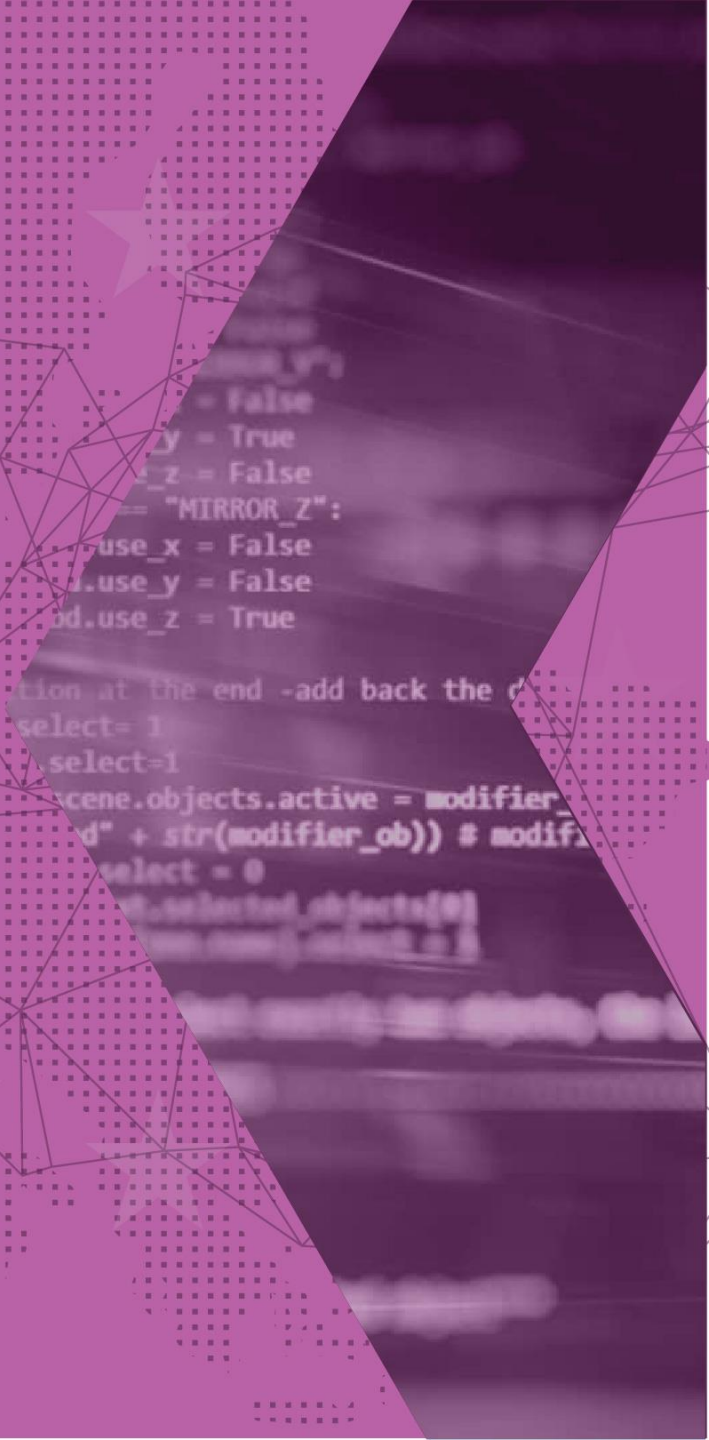
Článok 21 - Opatrenia na riadenie kybernetických rizík 2 vs V362

- zásady a postupy posudzovania účinnosti opatrení na riadenie kybernetických rizík; **§17c**
- základné postupy kybernetickej hygieny a odborná príprava v oblasti kybernetickej bezpečnosti; **§7**
- zásady a postupy používania kryptografie, prípadne šifrovania; **§17a**
- bezpečnosť ľudských zdrojov, zásady kontroly prístupu a správu aktív; **§7, §8, §6**
- v prípade potreby používanie riešení viacstupňovej alebo kontinuálnej autentifikácie, zabezpečenej hlasovej, obrazovej a textovej komunikácie a zabezpečených systémov komunikácie v núdzových situáciách v rámci subjektu. **§17b**

LEAD YOUR BUSINESS PROTECTED

02/

Audit kybernetickej bezpečnosti

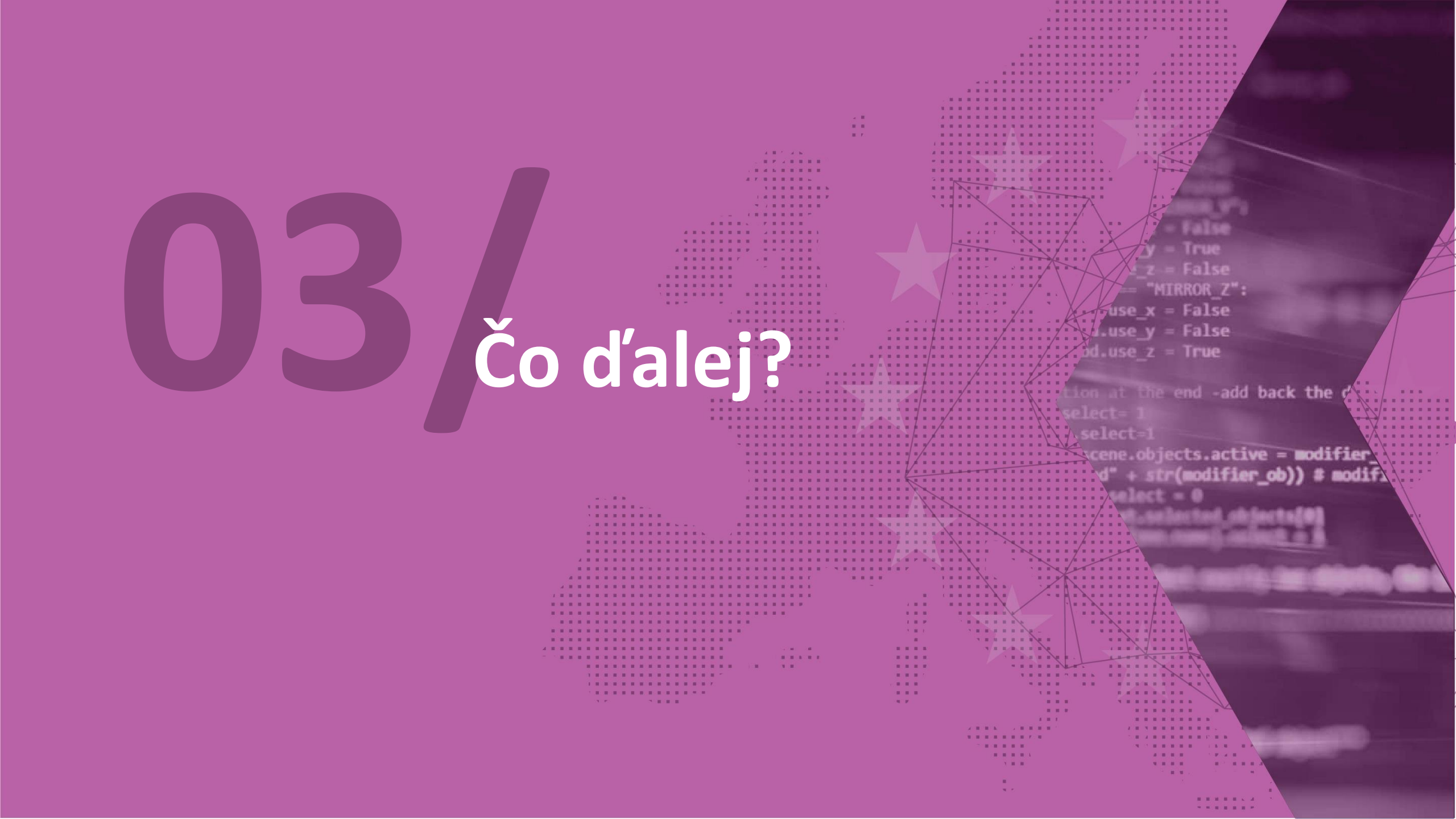


Audit kybernetickej bezpečnosti

- Povinnosť vykonať audit vyplýva priamo z NIS2.

LEAD
YOUR
BUSINESS
PROTECTED

03/ Čo ďalej?



Čo ďalej?

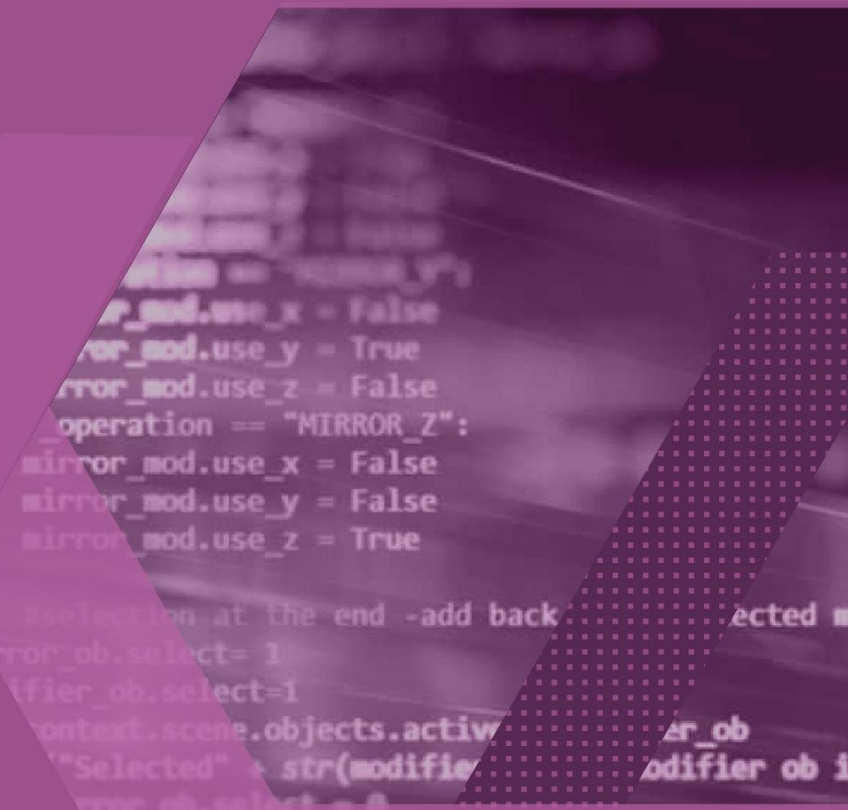
- Ste povinnou osobou v zmysle NIS2 (a novelizovaného ZoKB)?
  - Ak ste doteraz neboli PZS – porovnanie súčasného stavu voči aktuálne platnej legislatíve
- Aktívne sledovanie legislatívnych zmien v oblasti (stav novely ZoKB, aktualizácie príslušných vyhlášok NBÚ, prípadné relevantné sektorové vyhlášky....)
- Rozdielová analýza požiadaviek aktualizovaného ZoKB a príslušných vyhlášok.

LEAD
YOUR
BUSINESS
PROTECTED

cyllium

LEAD YOUR BUSINESS PROTECTED

Ďakujem za pozornosť



www.cyllium.eu