SECURITY DAYS

PRAKTICKÉ SKÚSENOSTI S AUDITOM PODĽA ZÁKONA O KYBERNETICKEJ BEZPEČNOSTI

Simona Salajová CISA, CISSP
ESET konzultant bezpečnosti a certifikovaný audítor ZoKB

Digital Security
Progress. Protected.

&

SME KONFERENCIE

Agenda

- Kto má povinnosť vykonať audit?
- Proces auditu
- Náležitosti a obsah auditu
- Nedostatky a zistenia počas výkonu auditov
- Ako vám vieme v ESETe pomôcť?

Kto má povinnosť vykonať audit?

- Prevádzkovateľ základnej služby (PZS) - do dvoch rokov odo dňa zaradenia PZS do registra prevádzkovateľov základných služieb.

- Každé dva roky - do dvoch rokov od vydania záverečnej správy o výsledkoch auditu.

- Pri každej významnej zmene - do dvoch mesiacov, odkedy má zmena významný vplyv na realizované bezpečnostné opatrenia.

Proces auditu, náležitosti, obsah

01

Kontaktovanie audítora

ŽIADOSTI O VYKONANIE AUDITU KYBERNETICKEJ BEZPEČNOSTI

02

Kick off/úvodné stretnutie:

i) ustanovenie spôsobu komunikácie

ii) identifikácia zodpovedných vlastníkov k oblastiam auditu

03

Priebeh auditu:

i) Stretnutia k jednotlivým oblastiam auditu

ii) Návšteva vybraných koncových bodov a ich audit z pohľadu fyzickej bezpečnosti

iii) Dodatočné požiadavky k vybraným oblastiam auditu (dodatočné dôkazy)

04

Ukončenie auditu

i) Návrh správy auditu na základe získaných dôkazov

ii) Pripomienky zástupcov PZS k auditným nálezom

iii) Vypracovanie vyjadrenia PZS k záverom auditu

iv) Odovzdanie finálnej správy PZS /**príprava harmonogramu opatrení k nálezom auditu zo strany PZS**

Náležitosti a obsah auditu

- Zákon č. 69/2018 Z. z.
- Bezpečnostná dokumentácia
- Stratégia kybernetickej bezpečnosti
- Klasifikácia a kategorizácia
- Oblasť podľa § 20 ods. 3 písm. a) zákona **organizácia kybernetickej a informačnej bezpečnosti**
- Oblasť podľa § 20 ods. 3 písm. b) zákona **riadenie rizík kybernetickej a informačnej bezpečnosti**
- Oblasť podľa § 20 ods. 3 písm. c) zákona **personálna bezpečnosť**
- Oblasť podľa § 20 ods. 3 písm. d) zákona **riadenie prístupov**
- Oblasť podľa § 20 ods. 3 písm. e) zákona riadenie **kybernetickej a informačnej bezpečnosti vo vzťahoch s tretími stranami**
- Oblasť podľa § 20 ods. 3 písm. f) zákona **bezpečnosť pri prevádzke informačných systémov a sietí**
- Oblasť podľa § 20 ods. 3 písm. g) zákona **hodnotenie zraniteľností a bezpečnostných aktualizácií**

Náležitosti a obsah auditu

- Oblasť podľa § 20 ods. 3 písm. h) zákona **ochrana proti škodlivému kódu**
- Oblasť podľa § 20 ods. 3 písm. i) zákona **sieťová a komunikačná bezpečnosť**
- Oblasť podľa § 20 ods. 3 písm. j) zákona **akvizícia, vývoja a údržba sietí a informačných systémov**
- Oblasť podľa § 20 ods. 3 písm. k) zákona **zaznamenávanie udalostí a monitorovanie**
- Oblasť podľa § 20 ods. 3 písm. l) zákona **fyzická bezpečnosť a bezpečnosť prostredia**
- Oblasť podľa § 20 ods. 3 písm. m) zákona **riešenie kybernetických bezpečnostných incidentov**
- Oblasť podľa § 20 ods. 3 písm. n) zákona **kryptografické opatrenia**
- Oblasť podľa § 20 ods. 3 písm. o) zákona **kontinuita prevádzky**
- Oblasť podľa § 20 ods. 3 písm. p) zákona **audit, riadenie súladu a kontrolné činnosti**
- **Manažér kybernetickej bezpečnosti** (§ 20 ods. 4 písm. a) zákona)

Nedostatky a zistenia počas výkonu auditov

90%

Personálna bezpečnosť

Riadenie kybernetickej a informačnej bezpečnosti vo vzťahoch s tretími stranami

80%

Riadenie prístupov

Sieťová a komunikačná bezpečnosť

Ochrana proti škodlivému kódu

70%

Riadenie rizík kybernetickej a informačnej bezpečnosti

Bezpečnosť pri prevádzke informačných systémov a sietí

Riešenie kybernetických bezpečnostných incidentov

Kontinuita prevádzky

40%+

Ostatné

Ako vám vieme v ESETe pomôcť?

Riadenie informačnej bezpečnosti

Pomôžeme Vám vylepšiť systém riadenia informačnej bezpečnosti a zvýšiť úroveň bezpečnosti v prostredí Vašej organizácie.

- Systém riadenia IB podľa normy ISO 27001
- Outsourcing bezpečnostného manažéra
- Analýza rizík
- BCM (Business Continuity Management)
- Bezpečnostný projekt na ochranu osobných údajov
- Tvorba vnútorných predpisov
- Konzultačná podpora
- Školenie kybernetickej bezpečnosti

Prejsť do sekcie Riadenie informačnej bezpečnosti ›

Bezpečnostný audit

Zhodnotíme stav informačnej bezpečnosti vo vašej organizácii a posúdime mieru súladu vášho informačného prostredia s legislatívou, odporúčaniami alebo dobrou praxou.

- Interný bezpečnostný audit
- Audit voči norme ISO 27002
- Audit voči platnej legislatíve
- Audit podľa Zákona o kybernetickej bezpečnosti
- GDPR audit
- Rýchly audit
- Sociálne inžinierstvo
- Penetračné testy
- ESET Vulnerability Assessment
- SWIFT Assessment

services@eset.sk

SECURITY DAYS

Ďakujem za pozornosť

Digital Security
Progress. Protected.

&

SME KONFERENCIE

SECURITY DAYS

Simona Salajová

ESET konzultant bezpečnosti a certifikovaný audítor ZoKB

simona.salajova@eset.com

Digital Security
Progress. Protected.

& SME KONFERENCIE