SECURITY DAYS

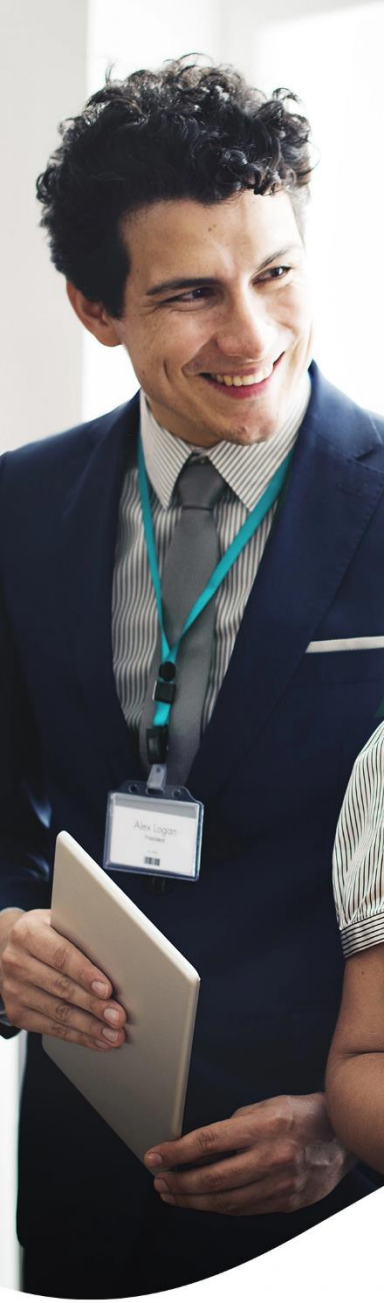
AKO ESET SERVICES POMÁHA ORGANIZÁCIÁM PRI ZABEZPEČOVANÍ SÚLADU S NOVELIZOVANÝM ZOKB

Simona Salajová
ESET Security Consultant, CISA, CISSP
a certifikovaný audítor ZoKB

Digital Security
Progress. Protected.

&

SME KONFERENCIE



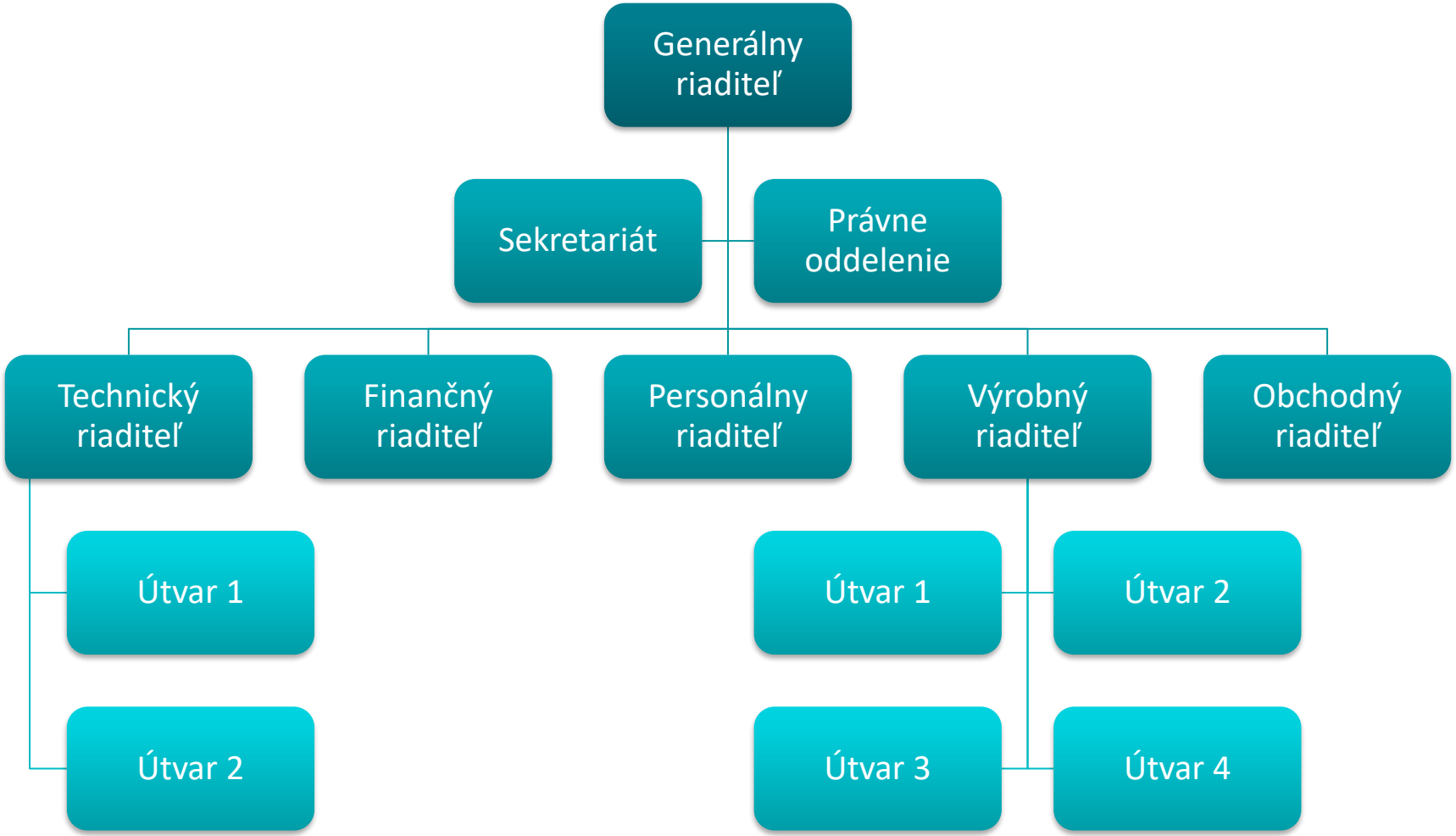
Ako vám vieme v ESETe pomôcť?

- Interný bezpečnostný audit
- Systém riadenia informačnej bezpečnosti podľa normy ISO27001
- Technický audit
- Školenie kybernetickej bezpečnosti
- Penetračné testy
- Testovanie metódou sociálneho inžinierstva
- Audit podľa Zákona o kybernetickej bezpečnosti č.69/2018
- GAP analýza existencie a vhodnosti dokumentácie s požiadavkami Zákona o kybernetickej bezpečnosti č.69/2018
- Zabezpečenie súladu s požiadavkami Zákona o kybernetickej bezpečnosti č.69/2018
  - Identifikácia a ohodnotenie aktív
  - Analýza rizík
  - Tvorba bezpečnostných politík a smerníc
- Konzultačná podpora

Identifikácia a ohodnotenie aktív a analýza rizík

- Úvodné stretnutie
- Identifikácia a ohodnotenie aktív
- Identifikácia hrozieb a zraniteľností
- Hodnotenie rizík
- Plán implementácie bezpečnostných opatrení
- Prezentácia výsledkov pre vedenie organizácie

Úvodné stretnutie



Identifikácia a hodnotenie aktív

Identifikácia aktív

- Primárne aktíva
- Podporné aktíva
- Vlastníci aktív
- Katalóg aktív

Hodnotenie aktív

- Dôvernosť
- Integrita
- Dostupnosť

Ako na identifikáciu a hodnotenie aktív – informácie/dáta

ID	Názov aktíva	Skupina aktív	Typ aktíva	Popis aktíva	Väzba/závislosť na ostatných aktívach	Lokalita/budova	Garant aktíva	Názov útvaru/ oddelenia
IA1	**Notebooky**	Hardware	Podporné aktívum	Notebooky zamestnancov				

Legislatívne/ regulatórne/ certifikačné požiadavky	Dodávatelia (vo vzťahu k aktívu)	Popis spolupráce	Dôvernosť	Integrita	Dostupnosť	Dôvernosť - oblasť dopadu	Integrita - oblasť dopadu	Dostupnosť - oblasť dopadu	RTO	RPO
GDPR			V	V	V					

Primárne aktívum

- Regulovaná služba podľa ZoKB
- Informačné/dátové aktíva a služby nutné pre zabezpečenie chodu organizácie (dáta o zákazníkoch/pacientoch/zamestnancoch, obchodné dáta, strategické informácie, know-how, technologické postupy, zdrojové kódy, …)

Podporné aktívum

- SW, webová aplikácia, služby
- HW (notebooky, stolné počítače, mobilné telefóny, servery, sieťové prvky, …)
- Ľudia (zamestnanci, dodávatelia)
- Sieť (LAN, VLAN)
- Priestory spoločnosti (dátové centrum, serverovňa, skrine, trezory, kancelárie, archív, …)

Analýza rizík

Identifikácia a hodnotenie hrozieb a zraniteľností

- Katalóg aktív
- Katalóg hrozieb
- Identifikácia a hodnotenie zraniteľností

Určenie miery rizík

- Register rizík
- Hodnotenie rizík
- Vlastník rizika

Rozhodnutie o spôsobe zvládania rizík

- Akceptácia
- Mitigácia
- Prenesenie alebo zdieľanie rizika
- Vyhnutie sa riziku

Plán implementácie bezpečnostných opatrení

- Prioritizácia
- Zodpovednosť
- Termíny

Definovať si metodiku

- Ako hodnotiť hrozby a zraniteľnosti
- Ako vypočítať mieru rizika

Katalóg hrozieb a zraniteľností

- Interné know-how
- Oblasti podľa ZoKB

Hodnotenie hrozieb a zraniteľností

Identifikácia a ohodnotenie hrozieb a zraniteľností						
Aktívum	**Skupina aktív**	**Hodnota aktíva**	**Hrozba**	**Hodnoty hrozby**	**Zraniteľnosť**	**Hodnota zraniteľnosti**
Notebooky	Hardware	V	Nevhodné nastavenie prístupových oprávnení / škodlivý kód	V	Bežní užívatelia majú účet lokálneho administrátora	V

Hodnota rizika = hodnota hrozby x hodnota zraniteľnosti x hodnota aktíva

Určenie miery rizík			
ID	**Riziko**	**Popis rizika**	**Hodnoty rizika**
R4	Nevhodné nastavenie prístupových oprávnení či zanesenie škodlivého kódu z dôvodu využívania práv lokálneho administrátora bežnými zamestnancami	Nevhodné nastavenie prístupových oprávnení či zanesenie škodlivého kódu z dôvodu využívania práv lokálneho administrátora bežnými zamestnancami (oddelenie obchodu, účtovné oddelenie)	V

Rozhodnutie o spôsobe zvládania rizík

Určenie miery rizík			Rozhodnutie o spôsobe zvládnutia rizika		
ID	**Riziko**	**Hodnoty rizika**	**Rozhodnutie o spôsobe zvládnutia rizika**	**Zdôvodnenie**	**Vlastník rizika (osoba zodpovedná za rozhodnutie)**
R4	Nevhodné nastavenie prístupových oprávnení či zanesenie škodlivého kódu z dôvodu využívania práv lokálneho administrátora bežnými zamestnancami	V	Zníženie rizika pomocou implementácie opatrení	Nevhodné nastavenie prístupových oprávnení či zanesenie škodlivého kódu z dôvodu využívania práv lokálneho administrátora bežnými zamestnancami	

Vybrané bezpečnostné opatrenia (stručný popis)
03 – Obmedziť práva bežných užívateľov alebo nastaviť kontrolné mechanizmy na monitoring ich činností pod účtami lokálneho administrátora

Plán implementácie bezpečnostných opatrení

Plán implementácie bezpečnostných opatrení						
ID	**Názov opatrenia**	**Popis spôsobu implementácie opatrenia**	**Priorita**	**Zodpovednosť za implementáciu opatrenia**	**Požadovaný termín implementácie**	**Aktuálny stav**

Terminológia

- Plán implementácie bezpečnostných opatrení = Plán zvládania rizík (podľa ZoKB)
  - Doplnené o nápravné opatrenia z auditu, námety na zlepšenia, …

Výhody

- Definované zodpovednosti
- Prioritizácia (podľa závažnosti identifikovaných rizík, logickej postupnosti, nadväznosti na projekty)
- Časový rámec (termíny)
- Stav jednotlivých bezpečnostných opatrení (projektové riadenie, využitie nástroja na riadenie úloh)
- Plánovanie rozpočtu a kapacít (náklady investičné, ľudské, prevádzkové)

Prezentácia výsledkov pre vedenie organizácie

- Prehľad rizík podľa závažnosti
- Presadzovanie ošetrenia rizík v organizácii

SECURITY DAYS

Simona Salajová

ESET Security Consultant, CISA, CISSP a certifikovaný audítor ZoKB

simona.salajova@eset.com

Obchod ESET Services

Email: services@eset.sk

Digital Security Progress. Protected. & SME KONFERENCIE