E-RAM

Enterprise Risk Analysis Manager

E B E European Business Enterprise

Průmyslový nástroj pro řízení kybernetické bezpečnosti

Systém E-RAM pro oblast průmyslových podniků je založen na dlouhodobě v praxi ověřeném systému RAM, který byl specificky upraven pro rozsáhlé implementace ve větších organizacích, řídících aktiva i rizika v různých oblastech, kdy jejich infrastruktura zahrnuje i průmyslové řídící systémy.

V řešení E-RAM získá podnik plnohodnotný produkt, který mu umožní řídit složitou problematiku kybernetické bezpečnosti v různých oblastech a sdílet informace napříč diverzifikovanými strukturami řízení podniků. Podniky jsou díky své velikosti a diverzifikaci procesů a protokolů snadné cíle. E-RAM umožňuje udržitelným a bezpečným způsobem vést proces celé kybernetické bezpečnosti napříč tímto heterogením prostředím.

S jeho pomocí si pro bezpečnostní týmy vytvoříte platformu, která Vám umožní jednoduchou správu a řízení aktiv, rizik a související bezpečnostní dokumentace napříč celým podnikem a v rúzných oblastech řízení bezpečnosti (fyzická, provozní, compliance, IT, OT atd.). Pomocí modudulů E-RAM můžete efektivně analyzovat zranitelnosti, rizika, plánovat opatření a vyhodnocovat jak jejich účinnost, tak i stav systému řízení bezpečnosti jako celku přes všechny oblasti a bezpečnostní týmy.

E-RAM je ve shodě se zákonem č. 181/2014 Sb., o kybernetické bezpečnosti, vyhláškou č. 82/2018 Sb., a zákonem č. 253/2008 Sb. o legalizaci výnosů z trestné činnosti (AML), směrnicí Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016, nařízením Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 (GDPR), nařízením Evropského Parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014, ČSN EN ISO/IEC 27001 Systémy managementu bezpečnosti informací – Požadavky, ČSN EN ISO/IEC 27005 Řízení rizik bezpečnosti informací, ČSN EN ISO/IEC 22301 Ochrana společnosti - Systémy managementu kontinuity podnikání - Požadavky, ČSN EN ISO/IEC 31000 Management rizik - Principy a směrnice, kdy pokrývá následující oblasti:

Řízení rizik informací

E-RAM Vám pomůže zavést procesy řízení rizik do Vašem podniku tak, aby nevytvářely negativní dopady, jako jsou složitá administrativa, vysoká cena bezpečnostních opatření, a aby Vám pomáhaly identifikovat existující zranitelnosti a efektivně na ně reagovat vhodnými a účinnými opatřeními. E-RAM Vám poskytne nástroje pro řízení rizik ověřené reálným provozem.

Řízení bezpečnosti informací

E-RAM Vám pomůže s vytvořením systému řízení bezpečnosti informací ve Vašem podniku, a to jak v oblasti řízení bezpečnosti informačních a průmyslových systémů, implementaci technologií, tak i při tvorbě bezpečnostní dokumentace a přípravě havarijních plánů. E-RAM Vám poskytnenástroje pro správu dokumentace, řízení aktiv a zavádění bezpečnostních opatření.

Řízení kontinuity činností

Při řízení kontinuity činností Vám E-RAM pomůže se zaměřit na kritické podnikové procesy,definovat aktivity pro snížení rizik vzniku rušivých událostí a zabezpečit tak kritické procesy při vzniku těchto události. E-RAM je účiným nástrojem pro vytváření strategií a plánů zachování kontinuity činností Vašich klíčových procesů a nástrojem pro zvládání rušivých událostí a sdílení krizových postupů.

Řízení kybernetické bezpečnosti

E-RAM Vám pomůže s vytvořením systému řízení kybernetické bezpečnosti ve Vašiem podniku dle platného právního rámce, a to jak při tvorbě bezpečnostní dokumentace a přípravě havarijních plánů, tak i při provozu a rozvoji Vašeho IT a OT. E-RAM Vám poskytne nástroje pro správu bezpečnostní dokumentace, řízení aktiv a zavádění bezpečnostních opatření.

Oblasti bezpečnosti

- ISO 27k
- ISO 22301
- ISO 31000
- Zákon č. 181/2014 Sb.
- GDPR
- AML

Funkcionality

- Modulární řešení
- Vlastní správa číselníků
- Volitelná struktura dat
- Nastavení pozadí položek
- Šablony dokumentace
- Vytváření vlastních sestav
- Nastavení vlastních vzorců
- Výpočty a hodnocení
- Dynamické animované grafy
- Filtry, vyhledávání, export
- Obesílání týmu

Šablony

- Katalog aktiv
- Katalog hrozeb, zranitelností
- Prohlášení o aplikovatelnosti
- Analýza rizik
- Plán opatření
- Hodnocení souladu

Komplexní číselníky

- ISO 27k
- ISO 22301
- ISO 31000
- Zákon č. 181/2014 Sb.
- GDPR
- AML

Individuální číselníky

- Důvěrnost
- Dostupnost
- Integrita
- Dopady
- Priorita
- Stav

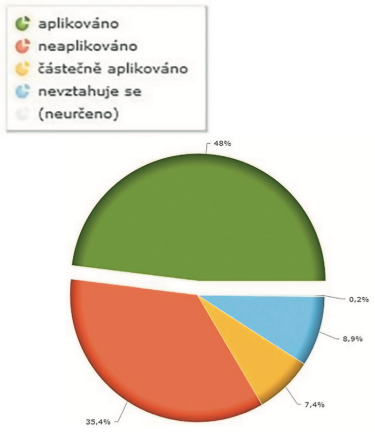
… a mnoho dalších

E-RAM
Enterprise Risk Analysis Manager

E B E European Business Enterprise

Opatření

	Bezpečnostní opatření	Stav	Odůvodnění / způsob implementace	Dokumentace
§ 3 a)	stanoví s ohledem na požadavky dotčených stran a organizační bezpečnost rozsah systému řízení bezpečnosti informací, ve kterém určí organizační části a aktiva, jichž se systém řízení bezpečnosti informací týká	aplikováno	Bezpečnostní politika	SM-BEZP-01
§ 3 b)	stanoví cíle systému řízení bezpečnosti informací	aplikováno	Bezpečnostní politika	SM-BEZP-01
§ 3 c)	pro stanovený rozsah systému řízení bezpečnosti informací na základě cílů systému řízení bezpečnosti informací, bezpečnostních potřeb a hodnocení rizik zavede přiměřená bezpečnostní opatření	částečně aplikováno	Probíhá redesign BP	
§ 3 d)	řídí rizika podle § 5	neaplikováno	Naplánováno vytvoření metodiky pro řízení rizik do 11/2018	ISO 31000
§ 3 e)	vytvoří a schválí bezpečnostní politiku v oblasti systému řízení bezpečnosti informací, která obsahuje hlavní zásady, cíle, bezpečnostní potřeby, práva a povinnosti ve vztahu k řízení bezpečnosti informací, a na základě bezpečnostních potřeb a výsledků hodnocení rizik stanoví bezpečnostní politiku v dalších oblastech podle § 30 a zavede přiměřená bezpečnostní opatření	částečně aplikováno	Probíhá redesign BP	
§ 3 f)	zajistí provedení auditu kybernetické bezpečnosti u informačního a komunikačního systému (dále jen „audit kybernetické bezpečnosti“) podle § 16	neaplikováno	Nebyl realizován, naplánován na 11/2018	
§ 3 g)	zajistí pravidelné vyhodnocování účinnosti systému řízení bezpečnosti informací, které obsahuje hodnocení stavu systému řízení bezpečnosti informací včetně revize hodnocení rizik, posouzení výsledků provedených auditů kybernetické bezpečnosti a dopadů kybernetických bezpečnostních incidentů na systém řízení bezpečnosti informací	neaplikováno	Neproběhlo, bude realizováno na základě 1. auditu organizace	
§ 3 h)	průběžně identifikuje a následně podle § 11 řídí významné změny, které patří do rozsahu systému řízení bezpečnosti informací	neaplikováno	Bude aktualizována Bezpečnostní politika	SM-BEZP-01



Aktivum	Riziko	Zranitelnost	Hrozba	Úr. dopadu	Úr. hrozby	Úr. zranitelnost	Úroveň rizika
Ekonomický systém (ERP)	R1	Známé chyby v programech	Zneužití oprávnění	Střední	Kritická	Kritická	Vysoké
LDAP	R2	Neprovádění logování událostí	Zneužití oprávnění	Vysoký	Vysoká	Vysoká	Vysoké
Osobní počítač	R3	Odcizení	Krádež zařízení	Střední	Nízká	Vysoká	Nízké
Nahrávací studio	R4	Odcizení	Krádež zařízení	Vysoký	Nízká	Kritická	Střední
Tiskárna Minolta TPKC	R5	Požár	Požár	Vysoký	Nízká	Nízká	Nízké
Datový portál	R6	Upgrade systému	Poškození dat	Vysoký			
Ekonomický systém (ERP)	R7	SW je již nepodporovaný - EOL	Chybné fungování aplikačního programového vybavení	Střední	Kritická	Střední	Střední
Kamerový systém	R8	Hrozí vandalismus a zneužití	Nezákonné zpracování dat	Střední	Vysoká	Střední	Střední

Business partner: