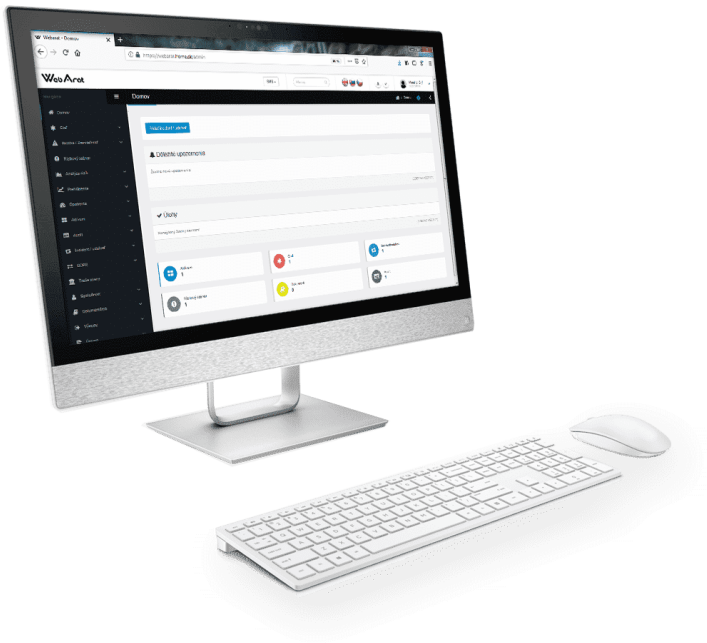
ALEF

WebArat

Informační systém pro evidenci, řazení procesů a dokumentace ISO norem, GDPR a kybernetické bezpečnosti



Je určený primárně pro manažery oblastí (normy, zákony), kteří potřebují mít přehled o všech svých povinných činnostech, aktivitách a zároveň mít nástroj, který je upozorní, pokud něco není zrealizované v požadovaném čase. Celý systém byl vytvořený na základě dobré praxe certifikačních auditorů, čímž se vytvořila struktura, kterou auditor při auditě potřebuje a není potřebné připravovat další dokumentaci potřebnou pro audit.

ISO normy

- **STN ISO/IEC 27001:2013 SMIB**
  Systém managementu informační bezpečnosti
- **STN EN ISO 9001:2015 SMK**
  Systém managementu kvality
- **STN EN ISO 14001:2005 EMS**
  Systém environmentálního managementu
- **STN EN ISO 45 001 OHSAS**
  Systém managementu bezpečnosti a ochrany zdraví při práci

Ochrana osobních údajů

Česká republika
Všeobecné nařízení o ochraně údajů (anglicky General Data Protection Regulation, zkratka GDPR).

Slovenská republika
Ve slovenském právním řádu je nařízení promítnuté do zákona č. 18/2018 Z. z. o ochrane osobních údajů a o změně a doplnění některých zákonů.

Legislativa

Česká republika
Zákon č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů.

Slovenská republika
Zákon č. 69/2018 Z. z. o kybernetické bezpečnosti a o změně a doplnění některých zákonů.

Trust the Strong

ALEF Distribution CZ, s.r.o. | Pernerova 691/42, 186 00 Praha 8, Česká republika | Phone: +420 225 090 240
cz-sales@alef.com | www.alef.com | twitter: @AlefSecurity

ALEF

Komponenty systému a metodika

Společnost

Základním prvkem organizačního řazení v systému je modul společnost. Je neoddělitelou součástí systému a obsahuje všechny nevyhnutelné náležitosti o společnosti. Jde o základní informace o společnosti, kontaktní informace, identifikační informace, organizační rozdělení a informace o zaměstnancích.

Struktura je rozdělená na tyto úrovně:

- Základní informace o společnosti,
- Organizační úseky,
- evidence zaměstnanců,
- skupiny rolí
- pracovní pozece.

Veškeré informace o zaměstnaních – osobní údaje jsou v databázi šifrované.

Informační aktiva

Informační aktiva – cokoliv, co má pro organizaci hodnotu. Existuje mnoho druhů aktiv včetně: a) informací; b) softwaru, jako je např. počítačový program; c) fyzických aktiv, jako je např. počítač; d) služeb; e) personálu a jeho kvalifikace, zručností a zkušeností; f) nehmotných aktiv, jako jsou např. pověst a image. Organizace identifikuje informační aktiva, její vlastníky, umístění aktiv, parametry, konkretizuje i požadavky na jejich vlastnosti, které je možné uspokojovat.

Proces kvality

Základným předmětom systému kvality je Proces. Proces je soubor vzájemně souvisejících nebo vzájemne se ovlivňujících činností, které transformují vstupy na výstupy. V organizaci nesmí existovat žádný proces, za který není nikdo zodpovědný. Každý proces musí mít související a návazné procesy, vstupy a výstupy do procesu, vazby na dodatele (pokud je to relevantní), vlastníka, operátora procesu, meřitelné výstupní parametry pro hodnocení výkonnosti procesu...

Environmentální aspekt

Základním předmětem systému enviromentálního managementu jsou Enviromentální aspekty, které určují jaké jsou hodnoty a jejich vliv na životní prostředí. Enviromentální aspekty se vztahují na činnosti a procesy organizace, které mohou mít pozitivní nebo negativní vliv na životní prostředí (např. vypuštění odpadových vod, emise a pod.).

Cíle a plány plnění cílů

Pro efektivní řízení systému je nevyhnutelné systém kontinuálně zlepšovat. Hlavním podkladem pro efektivní a kontinuální zlepšování systému je reálné a objektivní stanovení cílů, jejich plnění a objektivní vyhodnocení.

Je nevyhnutné, aby tvorba cílů vycházela z reálneho prostředí a ze zkušeností. Je důležité, aby cíle měly identifikovatalnou cílovou skupinu informačních aktiv/procesů/aspektů, pro které splnění cíle bude znamenat zlepšování systémů jako celku.

Proto je třeba stanovit:

- Hlavní prvky cílů informační bezpečnosti systému WebArat
- Určení cílů
- Plány plnění cílů
- Parametry na splnění cílů
- Vyhodnocování plnění cílů

Incidenty a události informační a kybernetické bezpečnosti

Povinnosti a zodpovědnosti

Základem pro účinné řazení incidentů a zlepšení informační bezpečnosti je přiřazení individuální zodpovědnosti za konkrétní činnosti. Cílem zavedení zodpovědnosti v managementu incidentů informační bezpečnosti musí být zabezpeční rychlé, efektivní a systematické odezvy na bezpečnostní incidenty.

Incident a událost informační bezpečnosti

Bezpečnostním incidentem je narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb nebo bezpečnosti a integrity elektronických komunikačních sítí v důsledků kybernetické bezpečnostní události. Bezpečnostní událostí je událost, která může způsobit narušení bezpečnosti informací v informačních systémech, narušení bezpečnosti služeb nebo bezpečnosti a integrity elektronických komunikačních sítí.

Zvládnutí informačních incidentů

Pro úspěšné zvládnutí incidentu informační bezpečnosti, odstranění hrozby, slabin a poučení se z nich, je potřebné vypracovat struktury, které postupným způsobem zabezpečí, že se rizika systematicky zlikvidují nebo se sníží na přijatelnou úroveň, respektive že budeme připravení na řešení incidentů.

Plány zvládnutí informačních incidentů a jejich oznámení

Měl by existovat systém hlášení o incidentech, slabinách, hrozbách a haváriích. Hlášení by měly směřovat od zaměstnanců k správcům systému až k bezpečnostnímu útvaru a příslušným orgánům. Oznamovací mechanismus by měl být jednoduchý (pochopitelný běžným uživatelem) a v závislosti na kritičnosti příslušně dostupný.

ALEF

Audity a kontroly

Auditorské činnosti jsou hlavním diagnostickým nástrojem managementu a fungují jako zpětná vazba poskytující informace o stavě systému organizace a procesů v nich probíhajících. Audity představují nezávislý zdroj informací a týkají se všech podnikových procesů, které tvoří efektivní a bezpečný systém organizace.

Audity systémů znamenají systematické a nezávislé zkoumání úrovně bezpečnosti s cílem určit, jestli činnost a související výsledky jsou v souladu s plánovanými zámery a jestli se této záměry realizují efektivně a jsou vhodné pro dosažení cílů. Na základě informací poskytnutých audity musí management přistoupit k potřebným opatřením vedoucím k zlepšování systému společnosti.

Hlavním cílem každého auditu musí být zjištění faktů, nikoli chyb. Ze zjištění auditu je potřeba vytvořit opatření:

- Řazení neshod
- Plány odstranění neshody
- Povinnosti a zodpovědnosti
- Parametry plnění cílů a jejich vazba na zjištění auditu
- Ověřování zavedených opatření

Rizikové scénáře

Modul **Rizikové scénáře** je základní modul na definování souvisejících vstupů do rizika. V rámci tohoto modulu se definují jednotlivé související vazby mezi aktivami / procesy / aspekty, podpornými aktivami, zavedenými opatřeními, a následně mezi hrozbami a zranitelnostmi / kořenovými příčinami.

Integrita systému je navrhnutá logikou, která nedovoluje v rámci aktiv/procesů/aspektů, podpůrných aktiv a zavedených opatření definovat vazby, které spolu nesouvisí. Tím se zabezpečuje správnost informací.

Vazby hrozeb a zranitelností/kořenových příčin s aktivami / procesy / aspekty, podpůrnými aktivami, zavedenými opatřeními musí identifikovat manager sám podle svých znalostí z reálného prostředí (nebo mu s tím pomůžeme v rámci implementace).

Způsob definování rizikových scénářů ve smyslu logiky systému nabízí různé způsoby přístupu k rizikovým scénářům či už na úrovni početnosti scénářů nebo na úrovni pohledu na hlavní předmět rizika.

Jako vstupy do řazení rizikových scénářů se využívají:
- aktiva/procesy/aspekty
- podpůrné aktiva
- katalog opatření, hrozeb a zranitelností

Rizikové scénáře jsou využívané i v rámci analýzy rizik, řazení auditních zjištění, či řazené incidentů a událostí.

Analýzy rizik

Analýza a ohodnocení rizik transformuje pohled na identifikování rizik prostřednictvím reálného ekonomického ohodnocení možných důsledků, ale také vyčíslení nákladů na realizaci opatření, které jsou potřebné na eliminování rizika. V této fázi existuje množství přístupů, ze kterých by si organizace měla vybrat vlastní, optimální kompromis mezi složitým výpočtem a jednoduchým odhadem. Organizace na které se vztahuje zákon o kybernetické bezpečnosti mají metodiku analýzy rizik přímo definovanou. Realistickým odhadem pravděpodobnosti reálnosti hrozby je možné sestavit například maticu míry rizika pro aktiva a odhadnout úroveň rizika.

Na základě úrovně rizika se potom lze rozhodnout, jestli je riziko přijatelné, nebo vyžaduje aplikovaní opatření. Ošetření rizik obsahuje i vyhodnocení nároků na aplikovaní opatření a jejich porovnání s mírou rizika a možnými důsledky pro organizaci pro realističtější hrozby. Organizace si pro rizika volí vědomě a objektivně přijatelnost rizika, vyhnutí se riziku aplikovaním opatření nebo přenesení rizika na třetí strany.

Hlavní prvky analýzy rizik systému WebArat:
- Metodika analýzy rizik podle požadavku zákazníka
- Akceptovatelná úroveň rizika
- Plán zvládnutí rizik
- Modifikovatelné úrovně kategorií a jejich nápočtů

Třetí strany

Evidence všech dodavatelů a odběratelů je vedená v module „třetí strany“. Obsahuje všechny nevyhnutelné náležitosti o společnosti. Jde o základní informace, kontaktní informace, identifikační informace, organizační rozdělení a informace o zaměstnancích a podobně.

Třetí strany jsou nevyhnutelnou součástí řazení rizik jako je evidence zodpovědností a povinností zabezpečovaných smluvními stranami. Třetí strany jsou integrované do všech modulů systému a v rámci jednotlivýcjh procesů jsou k nim definovaná práva, povinnosti a zodpovědnosti.

Dokumentace

Nevyhnutelným prvkem řazení je správná a aktuální dokumentace, která obsahuje všechny informace o zavedených procesech a opatřeních ve společnosti. Systém WebArt využívá na řazení dokumance oblasti systému jako například:

- Evidence dokumentace
- Řazení přístupu k dokumentaci
- Úloha / Práva a zodpovědnosti
- Vazba na Prohlášení o aplikovatelnosti
- Katalogy

V rozšířené verzi WebArt je k dispozici i systém pro tvorbu dokumentu a dokumentace, který je postavený na objektové tvorbě dokumentace s přesným procesným řazením a detailní politikou přístupu.

Výstupy

Modul výstupy představuje základní funkčnost na operativní zjišťování souvislostí a vazeb v rámci systému. Jde o zjednodušenou formu matice, která zajišťuje různé úhly pohledu definovaných struktur. Systém má v základě předdefinovanou základní strukturu vazeb a výstupů, které se v rámci implementace systému upravují podle požadavků zákazníka.

Trust the Strong

ALEF Distribution CZ, s.r.o. | Pernerova 691/42, 186 00 Praha 8,
Česká republika | Phone: +420 225 090 240
cz-sales@alef.com | www.alef.com | twitter: @AlefSecurity