



# WebArat

pravidlá vo vašich rukách

**Komplexný systém riadenia procesov  
kybernetickej bezpečnosti a GDPR**



## O systéme WebArat

- WebArat - nástroj pre evidenciu a riadenie oblastí kybernetickej bezpečnosti v logike a súlade ako to navrhuje a požaduje:
  - **ISO 27001**
  - **Zákon o kybernetickej bezpečnosti a súvisiace vyhlášky**
  - a hlavne **Best practice**
- Súčasťou systému je samostatný modul GDPR integrovaný do celkového riadenia kybernetickej bezpečnosti.

*Systém **WebArat** Vám ponúka možnosť mať prehľad a poznať súvislosti a na základe toho riadiť kybernetickú bezpečnosť a GDPR ako celok.*



# Pro koho je WebArat určený

- Primárne je určený pre **Manažéra kybernetickej bezpečnosti**
- Sekundárne pre:
  - Garantov primárnych a podporných aktív
  - Vedenie organizácie
  - Audítorov kybernetickej bezpečnosti
  - Správcov dokumentácie
  - DPO



# Oblasti riadenia v systéme WebArat

## Primárne oblasti riadenia

### Ciele kybernetickej bezpečnosti

- Plány plnenia cieľov

### Informačné aktíva

- Primárne aktíva (informácie, dáta, ...)
- Podporné aktíva (HW, SW, ľudia, ...)

### Bezpečnostné opatrenia

### Hrozby / zraniteľnosti

- Katalóg hrozieb
- Katalóg zraniteľností

### Tretie strany

### Analýza rizík

- Plány zvládania rizík
- Riziká
- Rizikové kombinácie

### Rizikové scenáre

- Definované hrozby
- Súvisiace zraniteľnosti
- Vybrané primárne aktíva
- Súvisiace podporné aktíva
- Súvisiace bezpečnostné opatrenia

## Sekundárne oblasti riadenia

### Incident / udalosť

- Incident / udalosť (evidencia)
- Plán zvládania incidentu / udalosti

### Audity

- Auditné zistenia
- Zvládanie auditného zistenia (úlohy)

### Kontrola

- Kontrolné zistenia
- Zvládanie kontrolného zistenia (úlohy)



# Oblasti riadenia v systéme WebArat

## Podporné oblasti riadenia

### Spoločnosť

- Evidencia zamestnancov
- Role
- Personálne skupiny rolí
- Organizačné úseky
- Pozície
- Budovy

### Dokumentácia

- Kompletná dokumentácia
- Tvorba / evidencia dokumentácie
- Pripomienkovanie
- Schvaľovanie
- Evidencia zmien
- Školenie a vzdelávanie

### GDPR

- Účely spracovania
- Evidencia súhlasov
- Evidencia žiadostí
- Poučenia a zmluvy
- Posúdenie rizikovosti / vplyvu
- Výstupy GDPR

### Výstupy

- OLAP pohľady
- Vlastné výstupy (tabuľky)
- Vlastné grafy

Prehlásenie o aplikovateľnosti

Úkolovník

Pracovné postupy (Workflow)

Upozornenia

Logy

Systémové role



# Možnosti implementácie systému WebArat

## Alternatíva 1

- implementácia súčasného stavu, metodík a postupov **bez našich doporučení**

## Alternatíva 2

- implementácia a **optimalizácia súčasných postupov** (súčasný procesy prejdú revíziou zo strany audítora a architekta kybernetickej bezpečnosti a na základe doporučení budú upravené)

## Alternatíva 3

- implementácia **celého systému riadenia kybernetickej bezpečnosti** (identifikácia a vyhodnotenie aktív, analýz rizík, spracovanie bezpečnostnej dokumentácie, bezpečnostných procesov apod.)



# Možnosti nasadenia

- WebArat je určený pre všetky typy organizácií a rôzne štruktúry riadenia
  - Základná – Manažér KB, ktorý má WebArat nasadený vo svojom pc /notebooku a kompletnú evidenciu a záznamy si riadi sám
  - Rozšírená - systém je nasadený v organizácii a pripája sa k nemu len úzky okruh kompetentných osôb
  - Kompletná - systém je nasadený v organizácii a pripájajú sa k nemu všetci zamestnanci, garanti aktív, riadiaci pracovníci a tiež zamestnanci, ktorí majú plniť jednotlivé úlohy, vzdelávajú sa, pripomienkujú alebo schvaľujú dokumentáciu, ...
- Možnosti nasadenia
  - On premise (doporučené pro rozšírené a kompletné nasadenie)
  - SaaS



## **Vybrané ukážky prostredia systému WebArat**







# Katalóg primárných aktív

Primární aktivum / Primární aktivum

Přidat Tiskový formulář Volba sloupců Export Tisk Nastavení

Počet záznamů: 10 Hledat: Hledej...



Zobrazuji 1 až 8 z celkem 8 záznamů < 1 >

Pořadové číslo	Název aktiva	Garant - organizační úsek	Důvěrnost	Integrita	Dostupnost	Typ aktiva	Kritický čas	Podpůrná aktiva
1	<a href="#">Služba connect</a>	IT oddělení	V Důvěrné informace	K Pro ochranu integrity dat...	K nevyhnutná dostupnost ...	Služba	1 hodina	10.4 Diesel generátor, 11 ...
2	<a href="#">Personální data</a>	Personální oddělení	V osobní údaje	V osobní údaje	S osobní údaje	Informace		1.1.2 Finance, 2.1 ms offic...
3	<a href="#">Heslá</a>		K Informace jsou vysoce ci...	K Aktivum je citlivé z hled...	K arušení dostupnosti aktiv...	Informace	4 hodiny	2.4 Keepass
3.1	<a href="#">Admin heslá</a>		K Informace nejsou veřejn...	K Aktivum je citlivé z hled...	K Narušení dostupnosti akt...	Informace	4 hodiny	2.4 Keepass, 9 Osoby / za...
3.2	<a href="#">Uživatelské heslá</a>		V Informace nejsou veřejn...	V Aktivum je citlivé z hled...	S Narušení dostupnosti akt...	Informace	8 hodiny	2.4 Keepass
4	<a href="#">Smlouvy</a>		V Informace nejsou veřejn...	V Aktivum je citlivé z hled...	S Narušení dostupnosti akt...	Informace	48 hodin	8.2 Budova A, 1.1.2 Finan...
5	<a href="#">Strategické smlouvy</a>	Company management	K Aktiva nejsou veřejně př...	V Aktivum vyžaduje ochra...	V Narušení dostupnosti akt...	Informace	24 hodin	2 Aplikace, 1.1.3 BI, 8.2 B...
8	<a href="#">Citlivá personální data</a>	Personální oddělení	K Aktiva nejsou veřejně př...	V Aktivum vyžaduje ochra...	V Narušení dostupnosti akt...	Informace	48 hodin	1.1.4 Systém BOZP

< 1 >











































# Katalog hrozieb

Hrozba / Hrozba  

[Přidat](#) [Zobrazit všechny](#) [Volba sloupců](#) [Export](#) [Tisk](#) [Nastavení](#)

Počet záznamů:  Hledat:

Zobrazuji 1 až 10 z celkem 17 záznamů [<](#) [1](#) [2](#) [>](#)

Pořadové číslo	Název	Popis	Incidenty	Auditní zjištění	Typ	Akce
1	porušení bezpečnostní politiky, proved...	porušení bezpečnostní politiky, proved...	Kategorie I – méně významný kybernet...	Neshoda (0), Pozorování (0)	Bezpečnostní	   
2	poškození nebo selhání technického a...	poškození nebo selhání technického a...	Kategorie I – méně významný kybernet...	Neshoda (0), Pozorování (0)	Bezpečnostní	   
3	zneužití identity,	zneužití identity,	Kategorie I – méně významný kybernet...	Neshoda (0), Pozorování (0)	Bezpečnostní	   
4	užívání programového vybavení v rozp...	užívání programového vybavení v rozp...	Kategorie I – méně významný kybernet...	Neshoda (0), Pozorování (0)	Bezpečnostní	   
5	škodlivý kód (například viry, spyware, tro...	škodlivý kód (například viry, spyware, tro...	Kategorie I – méně významný kybernet...	Neshoda (0), Pozorování (0)	Bezpečnostní	   
6	narušení fyzické bezpečnosti,	narušení fyzické bezpečnosti,	Kategorie I – méně významný kybernet...	Neshoda (0), Pozorování (0)	Bezpečnostní	   
7	přerušení poskytování služeb elektronic...	přerušení poskytování služeb elektronic...	Kategorie I – méně významný kybernet...	Neshoda (0), Pozorování (0)	Bezpečnostní	   
8	zneužití nebo neoprávněná modifikace...	zneužití nebo neoprávněná modifikace...	Kategorie I – méně významný kybernet...	Neshoda (0), Pozorování (0)	Bezpečnostní	   
9	ztráta, odcizení nebo poškození aktiva,	ztráta, odcizení nebo poškození aktiva,	Kategorie I – méně významný kybernet...	Neshoda (0), Pozorování (0)	Bezpečnostní	   
10	nedodržení smluvního závazku ze stran...	nedodržení smluvního závazku ze stran...	Kategorie I – méně významný kybernet...	Neshoda (0), Pozorování (0)	Bezpečnostní	   

[<](#) [1](#) [2](#) [>](#)



# Opatrenia - detail

Detail opatření

Seznam opatření / Detail opatření

Přidat poznámku Seznam poznámek Historie Duplikovat Upravit Smazat

Šifrování (ID 1)

Popis:	Encryption
Personální nastavení	
Autor:	Marek Uličný
Parametry	
Oblast:	ISMS, Kybernetický zákon SK, GDPR
Nadřazené opatření:	-
Pořadové číslo:	1
Hodnota:	100
Typy opatření:	Prevence
Vlastnosti informačnej bezpečnosti:	Důvěrnost, Integrita, Dostupnost
Koncepty kybernetickej bezpečnosti:	Ochrana
Prevádzkové schopnosti:	Bezpeční konfigurace
Bezpečnostné domény:	Ochrana
Dokumenty (Kapitoly):	Politika šifrování (ISMS/3_ver_1) 1 PRAVIDLA KRYPTOGRAFICKÉ OCHRANY INFORMACÍ 2 SYSTÉM SPRÁVY KLÍČŮ



# Rizikové scénáře - detail

## Detail rizikového scénáře

Seznam rizikových scénářů / Detail rizikového scénáře

Přidat poznámku Seznam poznámek + Riziková kombinace Duplikovat Upravit Smazat

### Rizikový scénář Výpadek elektrické energie (ID 4)

Základní popis rizikového scénáře:	Výpadek elektrické energie ze strany poskytovatele.
Oblast rizikového scénáře:	ISMS, Kybernetický zákon SK, GDPR
Dotčené aktiva:	Služba conect
Související podpůrné aktiva:	10.4 Diesel generátor, 11 Dodávateľ, 9.2 Správcí, 10.3 UPS 2
Zavedená opatření:	Řízený přístup, Monitorování a vyhodnocování, Šifrování, Redundance, Zálohování
Hrozba:	dlouhodobé přerušení poskytování služeb elektronických komunikací, dodávky elektrické energie nebo j
Zranitelnost:	nevhodná bezpečnostní architektura, zastaralost informačního a komunikačního systému,
Typ rizikového scénáře:	Bezpečnostní

#### Personální nastavení

Zodpovědný zaměstnanec:	Peter Michálek (008), Martin Gubov (009)
Autor:	Marek Uličný

#### Dátumy

Datum přidání:	19.11.2020
Datum úpravy:	20.12.2021
Datum uzavření:	

+ Riziková kombinace Duplikovat Upravit Smazat



# Vyhodnotenie rizika - detail

Detail analýzy rizik / Seznam analýzy rizik / Detail analýzy rizik

[Přidat poznámku](#) [Seznam poznámek](#) [Histórie](#) [Upravit](#) [Smazat](#)

[+ Přidat plán zvládání rizik](#)

**Analýza rizik pro rizikový scénář Kompromitácia hesiel (ID 1)**

Dopad		
Úroveň	%	Popis
Kritický	50	neplnení povinností

Zraniteľnosť		
Úroveň	%	Popis
Střední	10	služba není redundantná na potřebné úrovni

Hrozba		
Úroveň	%	Popis
Střední	21	Hrozba je málo pravdepodobná ale pravdepodobná.

Riziko		
Úroveň	%	Popis
Nízká / Akceptována	1	Riziko akceptováno

Ztráta důvěrnosti: ano

Ztráta integrity: ne

Ztráta dostupnosti: ano

Vazba na aktivum: Admin heslá, Heslá, Uživatelské heslá

Hrozba: pochybení ze strany zaměstnanců,

Zraniteľnosť: neschopnost včasného odhalení pochybení ze strany zaměstnanců.

Podpůrné aktiva: 2.4 Keepass, 9 Osoby / zaměstnanci, 9.2 Správci, 9.1 Uživatelé

Zavedené opatření: Vzdelávání, Šifrování, Řízený přístup, Monitorování a vyhodnocování



# Rizikovost'

WebArat ISMS Hledat... Marek Uličný superadmin

Navigace Riziko

- Analýza rizik
- Analýza rizik
- Plán zvládnání rizik
- Riziko**
- Rizikové kombinace
- Prohlášení
- Opatření
- Aktívum
- Audit
- Kontrola
- Incident / událost
- GDPR
- Třetí strany
- Společnost
- Dokumentace
- Výstupy
- Stupnice

Počet záznamů: 10 Hledat: Hledat...

Zobrazují 1 až 10 z celkem 288 záznamů

Riziko			Dopad			Hrozba			Zranitelnost:		
Rizikový scénář	Hodnota	Úroveň	Podpůrné aktivum	Hodnota	Úroveň	Hrozba	Hodnota	Úroveň	Zranitelnost	Hodnota	Úroveň
Kybernetický útok	27	V	Keepass	100	K	cílený kybernetický útok pomocl...	55	V	nehodná bezpečnostní archite...	50	V
Kybernetický útok	22	V	Production lan	80	K	cílený kybernetický útok pomocl...	55	V	nehodná bezpečnostní archite...	50	V
Kybernetický útok	22	V	Office lan	80	K	cílený kybernetický útok pomocl...	55	V	nehodná bezpečnostní archite...	50	V
Kybernetický útok	20	V	Virtuál BX1	75	K	cílený kybernetický útok pomocl...	55	V	nehodná bezpečnostní archite...	50	V
Kybernetický útok	19	V	windows server	70	K	cílený kybernetický útok pomocl...	55	V	nehodná bezpečnostní archite...	50	V
Kybernetický útok	19	V	Správci	70	K	cílený kybernetický útok pomocl...	55	V	nehodná bezpečnostní archite...	50	V
Kybernetický útok	16	V	Server B	60	K	cílený kybernetický útok pomocl...	55	V	nehodná bezpečnostní archite...	50	V
Únik citlivých dat	11	V	Keepass	100	K	cílený kybernetický útok pomocl...	55	V	nedostatečná údržba informační...	21	N
Únik citlivých dat	11	V	Keepass	100	K	cílený kybernetický útok pomocl...	55	V	Nedostatečný algoritmus šifrova...	20	N
Kybernetický útok	11	V	Keepass	100	K	cílený kybernetický útok pomocl...	55	V	nedostatečná údržba informační...	21	N



# Výstupy systému WebArat

Domů

Cíl

Hrozba / Zranitelnost

Rizikový scénář

Analýza rizik

Prohlášení

Opatření

Aktivum

Audit

Kontrola

Incident / událost

GDPR

Třetí strany

Společnost

Dokumentace

Výstupy

**Primární aktivum**

Podpůrné aktivum

Hrozba

Zranitelnost

Analýzy rizik

Zavedená opatření

Primární aktivum \*

Oblast \*

Podpůrné aktiva  Incidenty/události  Auditní zjištění

Rizikové scénáře  Hrozba  Zranitelnost  Analýzy rizik

Zavedená opatření

Zobrazit

Primární aktivum	Oblast	Požadavek na výstup	
Heslá	Podpůrné aktiva	Keepass	
	Incidenty/události	Není definováno	
	Auditní zjištění	Není definováno	
	Rizikové scénáře	Kompromitácia hesiel, Kybernetický útok, Únik citlivých dat	
	Hrozba		pochybení ze strany zaměstnanců, porušení bezpečnostní politiky, provedení neoprávněných činností, zneužití oprávnění
			poškození nebo selhání technického anebo programového vybavení,
			cílený kybernetický útok pomocí sociálního inženýrství, použití špionážních technik, napadení elektronické komunikace (odposlech, modifikace).
	Zranitelnost		nedodržení smluvního závazku ze strany dodavatele, nedostatek zaměstnanců s potřebnou odbornou úrovní,
			neschopnost včasného odhalení pochybení ze strany zaměstnanců. Nedostatočný algoritmus šifrovania
	Analýzy rizik		nedostatečná údržba informačního a komunikačního systému, nevhodná bezpečnostní architektura, nevhodné nastavení přístupových oprávnění, nedostatečné bezpečnostní povědomí uživatelů a administrátorů,
Zavedená opatření		Kybernetický útok (Dopad by měl být plošný rozsahem, trvalý a katastrofický. Rozsah případných škod přesahuje 3 000 000 €, Hrozba je pravděpodobná až velmi pravděpodobná., Zranitelnost je málo pravděpodobná ale nepravděpodobná., Riziko je dlouhodobě nepřijatelné a musí být zahájeny systematické kroky k jeho odstranění.)	
		Šifrování, Redundance, Řízený přístup, Zálohování, Monitorování a vyhodnocování	





## Záver

Celkový výsledok práce so systémom WebArat má priniesť prehľad a schopnosť či už preventívne alebo reaktívne reagovať na potenciálne hrozby (a určite i poskytnúť komplexné informácie o riadení pri kontrolách a auditoch KB).

Ďakujem za pozornosť

Ing. Marek Uličný

Slovenská republika:		Česká republika:
<b>WebArat Solutions, s.r.o.</b> (+421) 948 834 347 <a href="mailto:webarat@webarat.sk">webarat@webarat.sk</a>	<b>SophistIT, s.r.o.</b> (+421) 2 20 62 06 70 <a href="mailto:info@sophistit.com">info@sophistit.com</a>	<b>Alef NULA, a.s.,</b> (+420) 702 259 478 <a href="mailto:radek.svadlenka@alef.com">radek.svadlenka@alef.com</a>