



# Řízení kybernetické bezpečnosti online a datový audit

Ing. Vojtěch Hvězda



# PDIL (Personal Data & Identity Lookup)

Nástroj vhodný pro datový audit v organizaci. Jedná se o pro pokročilé vyhledávání osobních údajů a dalších typů údajů v souborových dokumentech a databázích a jejich klasifikace. PDIL dokáže na základě vyhledaných dat udělat automatickou či manuální anonymizaci těchto dat.

## Přínosy:

- Jasná a přesná identifikace osobních údajů
- Značení dokumentů s osobními údaji
- Vlastní báze vyhledávaných
- Učení vlastních šablon dokumentů
- Moderní grafické přehledy a práce s nimi
- Anonymizace dat





# PDIL – Anonymizace

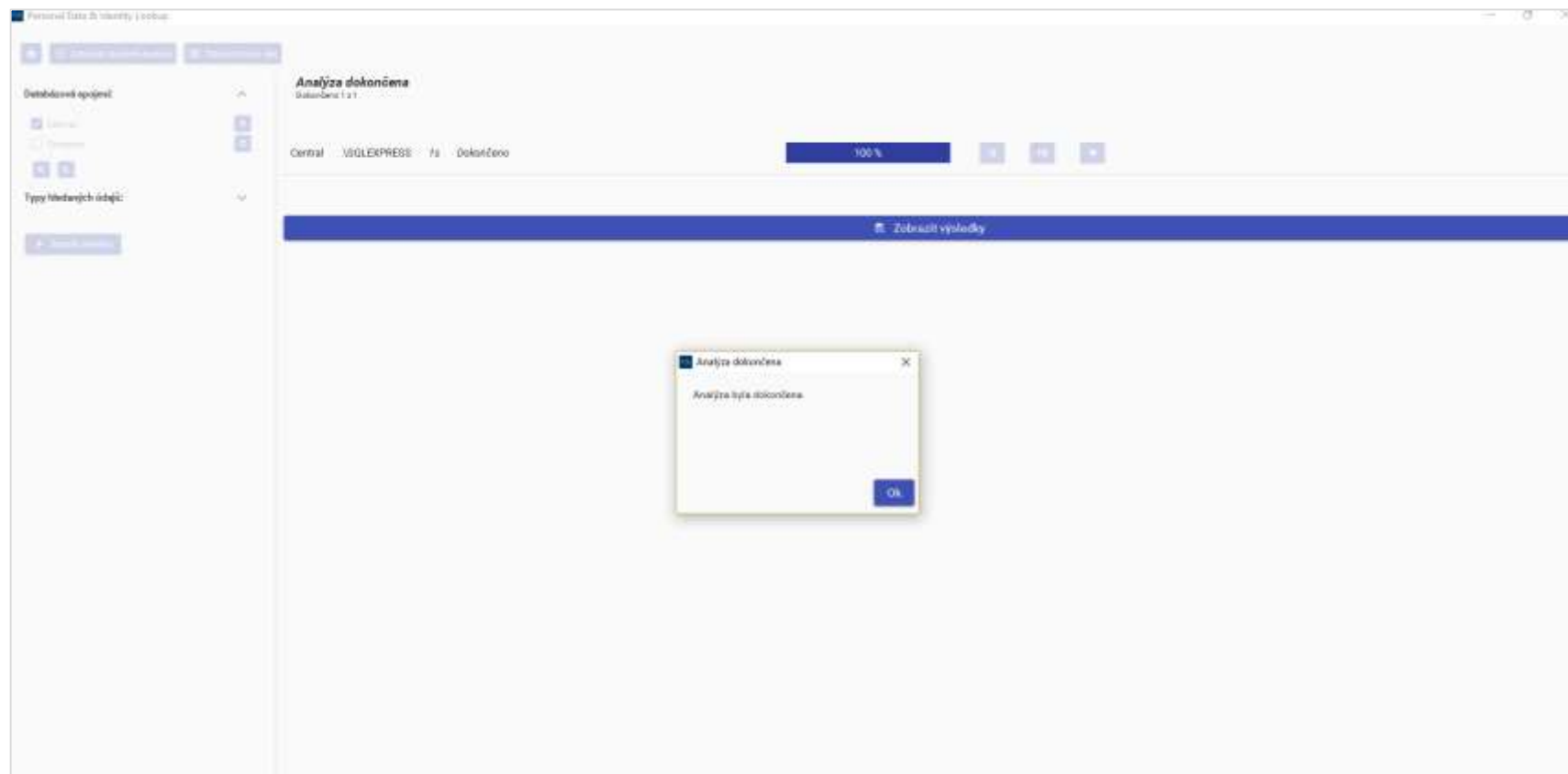
## Výstup

The screenshot displays a file management application interface. On the left, there is a sidebar with navigation options like 'Typy souborových zdrojů' and 'Typy klíčových údajů'. The main area shows a table of files with columns for 'Název souboru', 'Datum změny', 'Datum vytvoření', and 'Adresa'. A dialog box is overlaid on the table, asking 'Opravdu chcete automaticky anonymizovat 4 soubory?' with 'Ano' and 'Ne' buttons. Below the table, there are search filters and a summary section titled 'Vybíráte 4 soubory' with a 'Vše' button and a checkbox 'Zahrnout anonymizované soubory?'. A warning message states: 'Soubory DOC se načítají jako soubory DOC a PDF jako PDF. Žluté soubory ještě anonymizovat.'

	Název souboru	Datum změny	Datum vytvoření	Adresa
10	Ostatky semestr.docx	7.12.2017 16:40:06	7.12.2017 16:40:06	C:\Users\kresa\Desktop\Ústav
11	Pařížky.docx.docx	20.3.2018 08:55:27	20.3.2018 08:55:28	C:\Users\kresa\Desktop\Ústav
12	Prof. Malal.docx	8.11.2017 07:58:43	7.11.2017 18:44:38	C:\Users\kresa\Desktop\Ústav
13	Přehledy_druhů_revizce.pptx	28.10.2017 18:03:25	25.10.2017 18:03:25	C:\Users\kresa\Desktop\Ústav
14	Připrava 5.docx	14.1.2018 10:28:33	23.10.2017 14:05:38	C:\Users\kresa\Desktop\Ústav
15	Souvislosti.docx	16.12.2017 17:43:01	16.12.2017 18:02:56	C:\Users\kresa\Desktop\Ústav
16	Výsledky na Měnové.docx	25.11.2018 13:25:04	15.11.2017 12:17:00	C:\Users\kresa\Desktop\Ústav
17	Úvodní informace.docx		8.10.2017 16:47:51	C:\Users\kresa\Desktop\Ústav
18	Kresa-MVZ402-Seminář 10.docx		27.11.2017 21:12:51	C:\Users\kresa\Desktop\Ústav\Gepořtkita
19	Kresa-MVZ402-Seminář 11.docx		30.11.2017 08:57:38	C:\Users\kresa\Desktop\Ústav\Gepořtkita
20	Kresa-MVZ402-Seminář 12.docx		1.12.2017 13:18:56	C:\Users\kresa\Desktop\Ústav\Gepořtkita
21	Kresa-MVZ402-Seminář 13.docx		3.12.2017 16:23:39	C:\Users\kresa\Desktop\Ústav\Gepořtkita
22	Kresa-MVZ402-Seminář 2.docx	11.1.2018 16:24:28	3.10.2017 16:32:54	C:\Users\kresa\Desktop\Ústav\Gepořtkita
23	Kresa-MVZ402-Seminář 3.docx	18.10.2017 12:18:46	18.10.2017 12:18:46	C:\Users\kresa\Desktop\Ústav\Gepořtkita

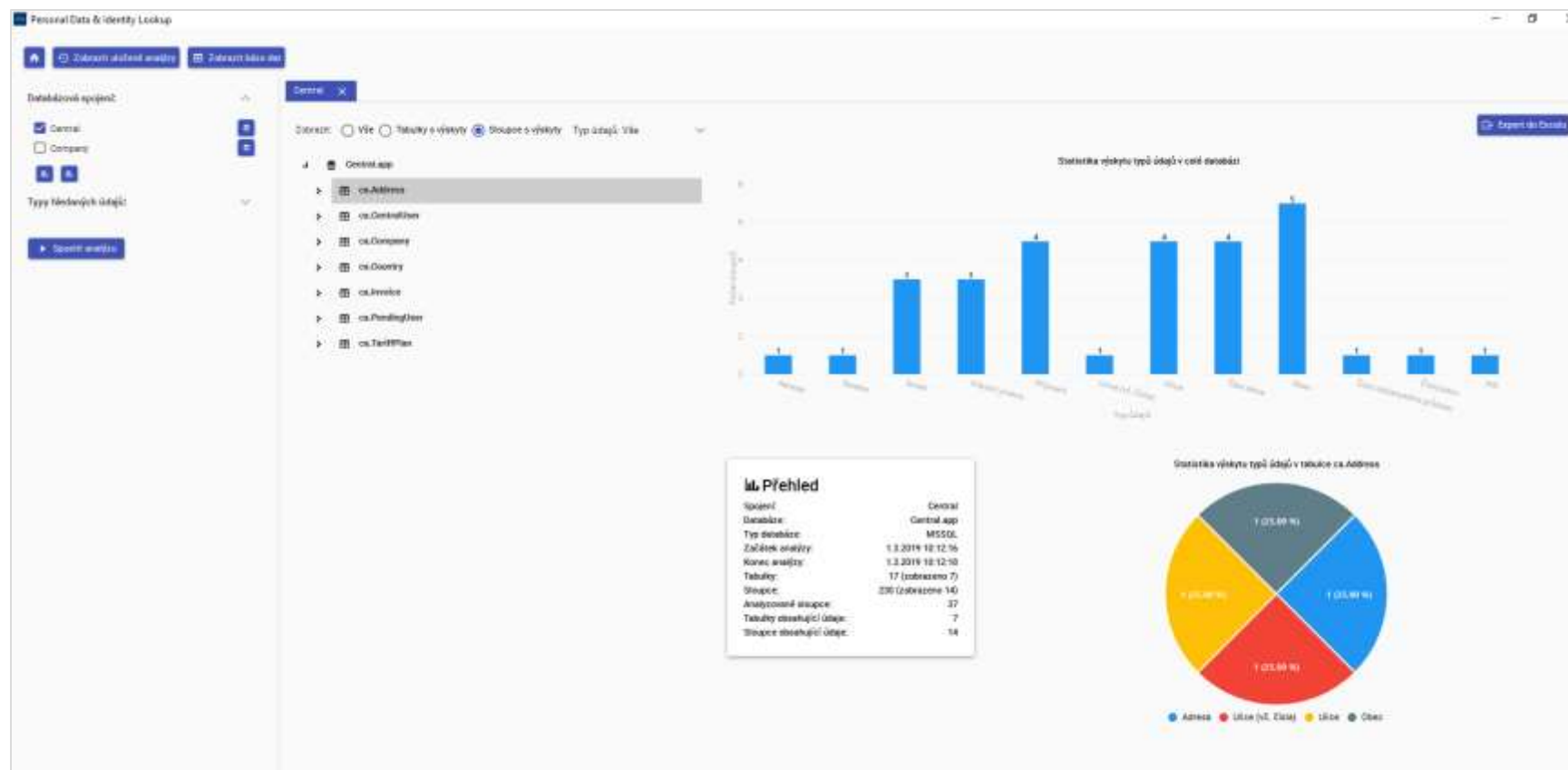
# PDIL – Prohledání DB

Výstup



# PDIL – Prohledání DB

Výstup



# CSA (Cyber Security Audit)

## Identifikace a řízení Aktiv

Identifikace a řízení aktiv, customizace pro jednotlivé typy zákazníků, dle charakteru jejich interní metodiky. Systém poskytuje pokročilé importy pro možnosti integrace již vytvořených přehledů. CSA obsahuje všechny náležitosti, které vyžaduje legislativa ČR pro toto téma.

## Řízení rizik

Na základě výsledků hodnocení jednotlivých aktiv je postaven mechanismus řízení rizik. Obsahuje analýzu rizik, prohlášení o aplikovatelnosti jednotlivých opatření a samotný plán zvládnutí rizik s pokročilými metodami distribuce řešitelům (garantům aktiva), včetně zpětné vazby a řešitelského logu.

## Interní audit kybernetické bezpečnosti

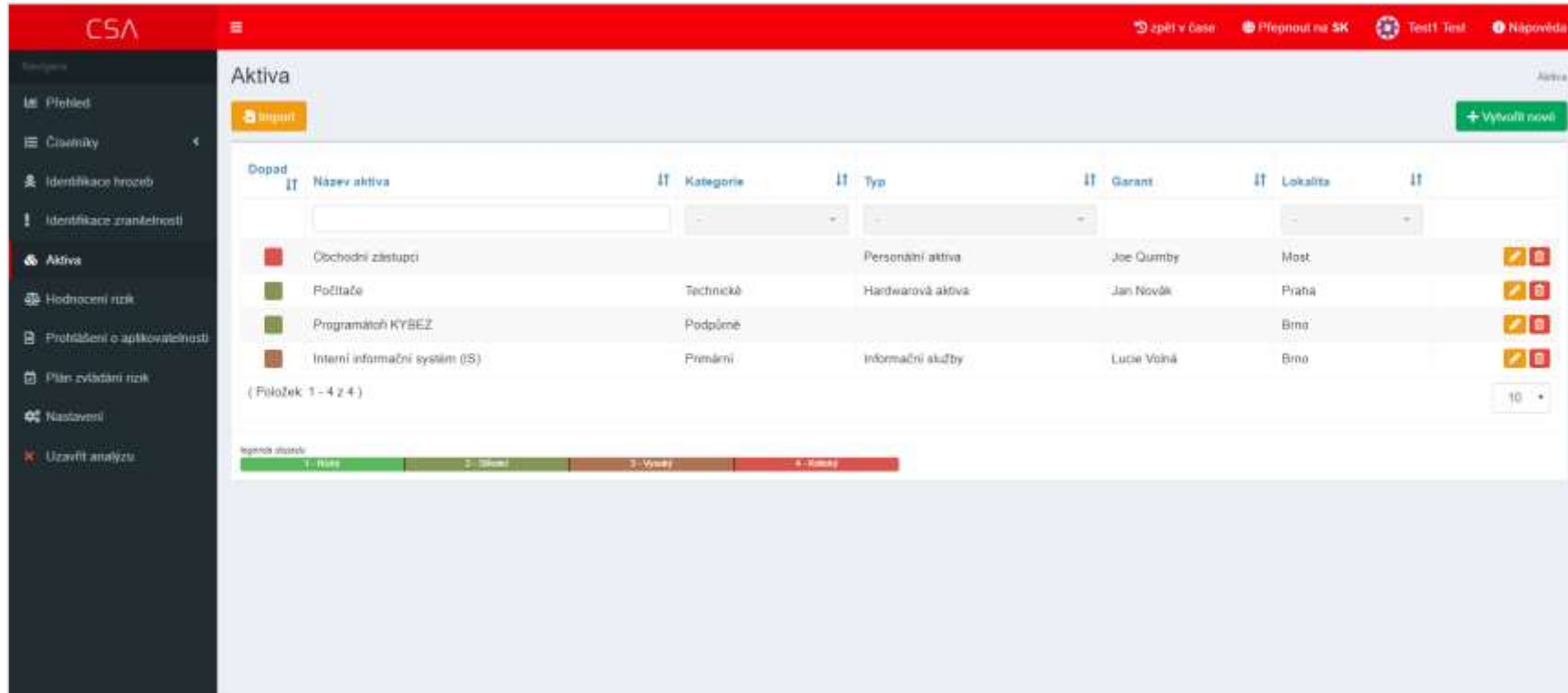
Je možné provést interní audit, který vychází z doporučení NBÚ.





# CSA – Přehled aktiv

Výstup



CSA

zpět v čase Přepnout na SK Test1 Test Návod

Aktiva

Import + Vytvořit nové

Dopad	Název aktiva	Kategorie	Typ	Garant	Lokalita	
	Obchodní zástupci		Personální aktiva	Joe Qumby	Most	
	Počítače	Technické	Hardwarová aktiva	Jan Novák	Praha	
	Programátch KYBEZ	Podpómě			Brno	
	Interní informační systém (IS)	Přímáří	Informační služby	Lucie Vohná	Brno	

( Položek 1 - 4 z 4 )

10

legenda stavů: 1 - Nízké 2 - Střední 3 - Vysoké 4 - Kritický

# CSA – Definice hrozeb

Výstup

The screenshot displays the CSA web application interface for threat identification. The top navigation bar is red and contains the 'CSA' logo, a menu icon, and several utility buttons: 'zpět v čase', 'Přepnout na SK', 'Test1 Test', and 'Nápověda'. The left sidebar is dark grey and lists various navigation items: 'Přehled', 'Časovky', 'Identifikace hrozeb' (highlighted), 'Identifikace zranitelnosti', 'Aktiva', 'Hodnocení rizik', 'Prohlášení o aplikovatelnosti', 'Plán zvládnutí rizik', 'Nastavení', and 'Uzavřít analýzu'. The main content area is titled 'Identifikace hrozeb' and features a 'Typy hrozeb' section with a search input field labeled 'název' and a '+ nový' button. Below this is a table listing threat types: 'Kybernetické útoky', 'Lokální', 'Ostatní', 'Přírodní', and 'Ztráta většího (kritického) množství pracovníků'. Each row has edit and delete icons. To the right of the table is a vertical list of five green boxes representing threat categories: 'Kybernetické útoky', 'Lokální', 'Ostatní', 'Přírodní', and 'Ztráta většího (kritického) množství pracovníků', each with a plus sign and a minus sign icon.

# CSA – Přehled rizik

Výstup

The screenshot displays the 'Hodnocení rizik' (Risk Assessment) interface. The table lists various risks with columns for 'Aktivum', 'Druh hrozby', 'Druh zranitelnosti', 'Dopad', 'Hrozba', 'Zranitelnost', 'Riziko', 'Akceptováno', and 'Opatření'. A progress bar at the bottom indicates the status of risk classification.

Aktivum	Druh hrozby	Druh zranitelnosti	Dopad	Hrozba	Zranitelnost	Riziko	Akceptováno	Opatření
Obchodní zástupce	Hromadný odchod	Neschopnost zajistit po lidské stránce chod systému						
Počítače	Malware (různé druhy)	Nedostatečně či zastaralé bezpečnostní systémy	Nízký	Vysoká	Nízká	Vysoká (70%)	ne	
Server HP	Man-in-the-Middle	Nedostatečně či zastaralé bezpečnostní systémy						
Programátoři KYBEZ	Hromadný odchod	Neschopnost zajistit po lidské stránce chod systému						
Interní informační systém (IS)	DoS/DDoS	Nedostatečně či zastaralé bezpečnostní systémy					ne	

( Položek: 1 - 5 z 5 )

Agenda klasifikace rizik

0% 10% 20% 30% 40% 50% 60% 70% 80% 90% 100%

[www.gordiccybersec.cz](http://www.gordiccybersec.cz)



Děkuji za pozornost

