

GDPR ve Vaší organizaci.

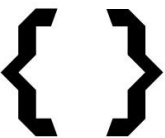
Nestrašíme, pomáháme

Jiří Stich
Člen výkonného výboru CSCC



Atos

Stávající členové CSCC



Univerzita Hradec Králové





Vznik a poslání klastru

- ▶ CSCC byl založen 15.12.2015
- ▶ Zakládající členové
 - Atos IT Solutions and Services, Česká Spořitelna, ČVUT, E.ON, Schneider Electric a Technologické centrum Písek
- ▶ Poslání
 - Rozvoj jedinečného partnerství mezi firmami, státní správou, samosprávou, znalostními institucemi a obyvateli měst
 - Pomoc vedení měst a krajů s přípravou inovativních konceptů
 - Dohled nad realizovanými projekty
 - Vytvoření srozumitelné metodiky

— GDPR - strašák nebo příležitost?

1. Plníte (snažíte se) 122/2013 Z.z. a 164/2013 Z.z. ?
Pak je GDPR jen trocha práce navíc (nové instituty)
2. Je pro Vás ochrana OÚ a ISO 27001 pouhé intelektuální cvičení?
Pak Vás čeká dost práce
3. Je motivací stran GDPR tlak „zeshora“, nebo se obáváte svých
zákazníků / dodavatelů / partnerů?
4. Zkusíte to sami, nebo s podporou Atosu? 😊

1 Právní analýza

2 Revize procesů

3 Datový audit

4 Report a návrh nápravných opatření

5 Zavádění opatření

1 Právní analýza

Tipy a Triky, na co si dát pozor

Právní (prvotní, dopadová) analýza by ruku v ruce měla jít s analýzou rizik.

A to jako proč?

Deklarovaný soulad s legislativou prostřednictvím skvěle zpracované, ale **v prostředí nezavedené** bezpečnostní politiky v organizaci se organizaci vymstí v podobě neschopnosti procesovat požadavky subjektů OÚ.

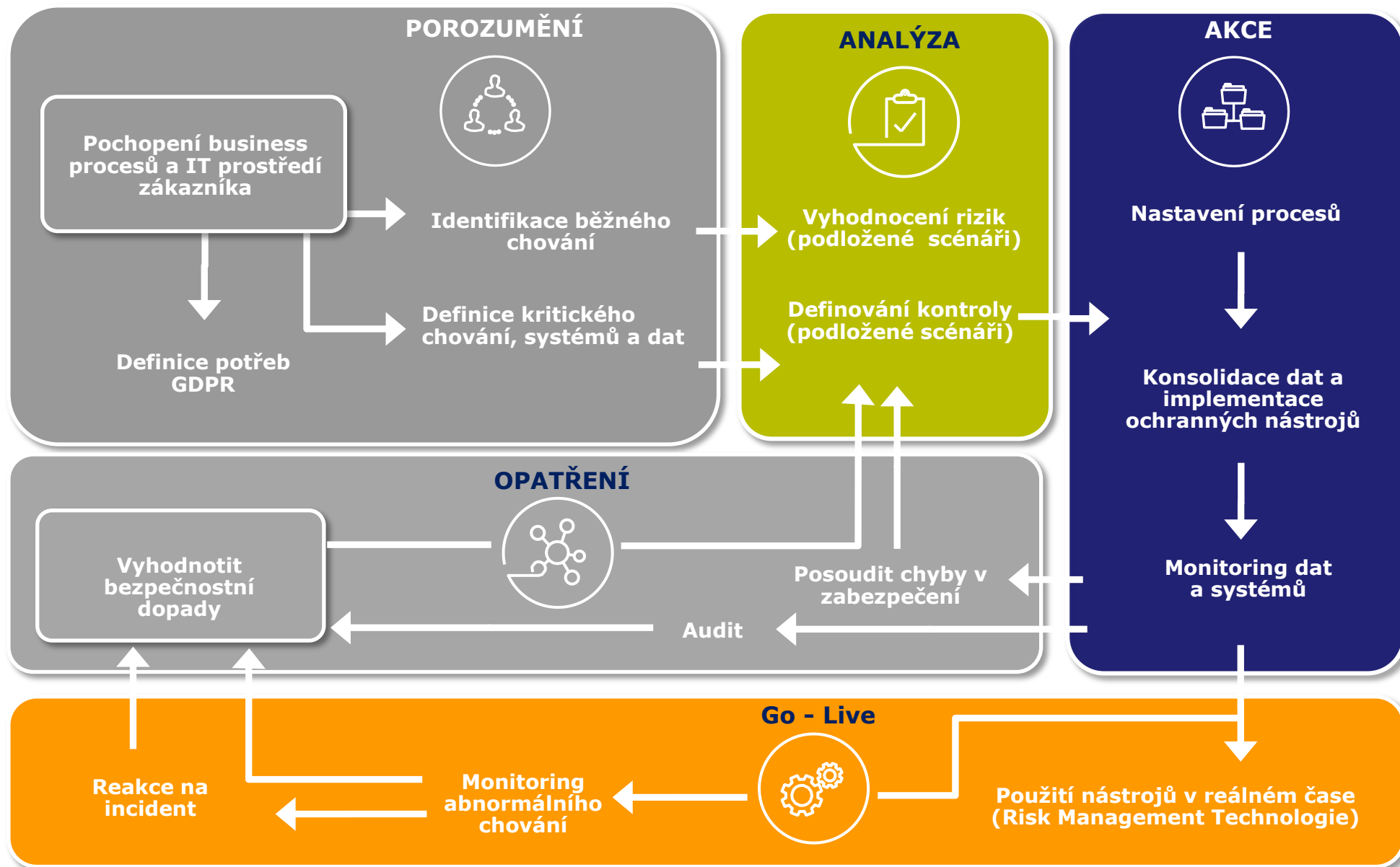
#	Požadavek	Ano	Ne	Částečně
1	Je zabezpečena ochrana perimetru Firewalllem?	X		
2	Je zpracovaný akt formou směrnice stran řízení přístupu k informačním systémům?	X		
3	Máte vytvořenu politiku klasifikace dokumentů?	X		

A v reálném prostředí to vypadá jak?

2

Revize procesů

Máte popsány, nebo alespoň zmapovány Vaše procesy?



3

Datový audit

Hodnocení rizik GDPR dat

5 jednoduchých otázek

1. Jaká osobní data občanů EU máte v držení?
2. Jak citlivá data to jsou?
3. Kde se v rámci organizace tato nacházejí a kdo k nim přistupuje?
4. Jak se v organizaci pohybují, kam a kudy z organizace odcházejí?
5. Jak se s nimi pracuje a komu jsou poskytována?

Fáze 1 - Analýza statických dat

Poznejte, kde jsou uložena Vaše osobní data

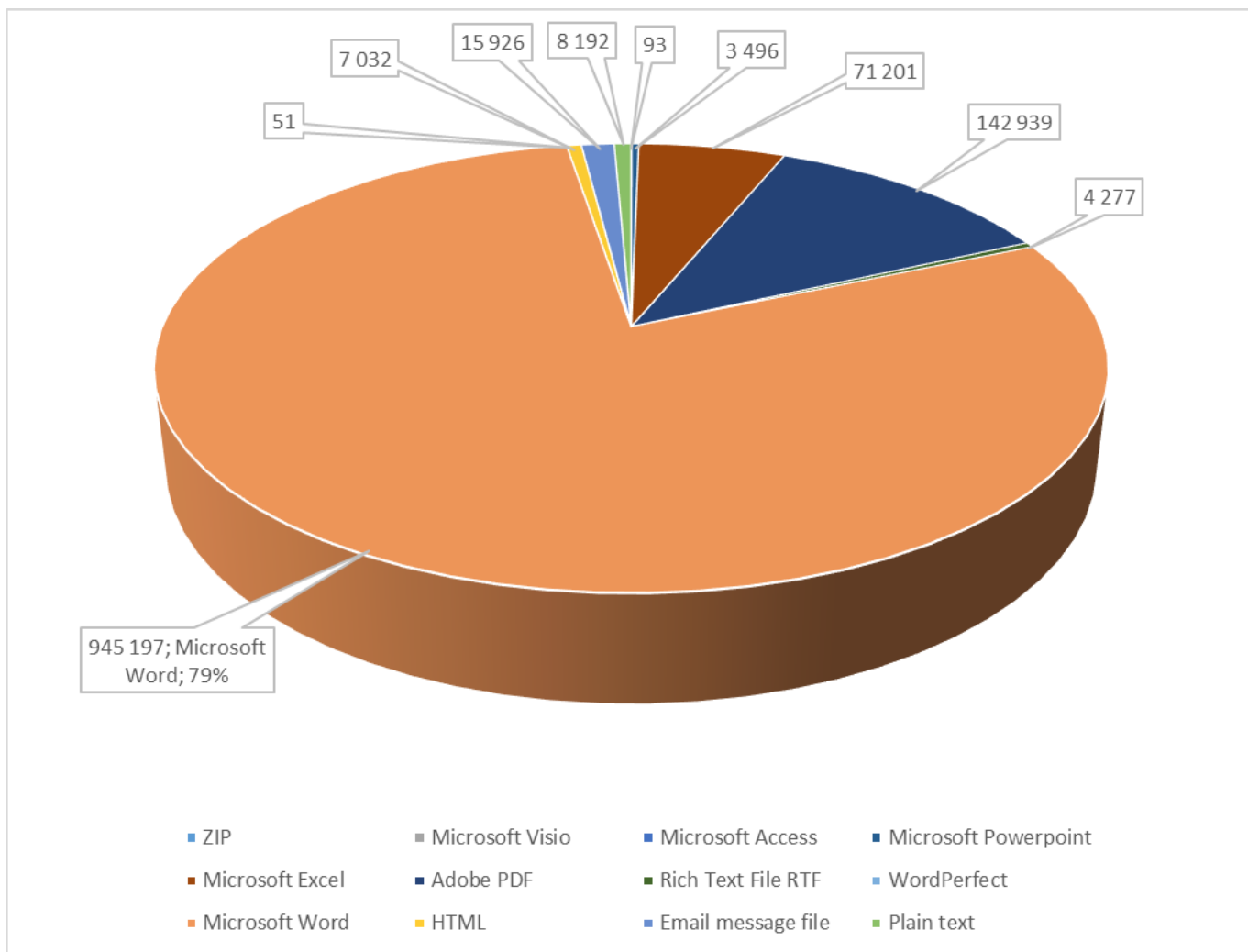
Tato analýza zahrnuje zjištění, detekování osobních dat občanů EU napříč Vaší datovou infrastrukturou, tedy síťovými úložišti, databázemi a cloudovými úložišti. Naše platforma má vestavěné politiky detekující datové vzory GDPR, nemusíte je tedy složitě definovat. Vlastní vzory GDPR dat typické pro Vaši organizaci Vám rádi nastavíme a budeme schopni detekovat jejich přítomnost jak na lokálních, síťových i cloudových úložištích.

Naše platforma „ATOS threat aware data protection“ skenuje úložiště, která určíte za účelem identifikace:

- Všech typů osobních dat
- Úrovní citlivosti těchto dat
- Která úložiště obsahují osobní data



Číslo z praxe – v jakých datech nacházíme osobní údaje



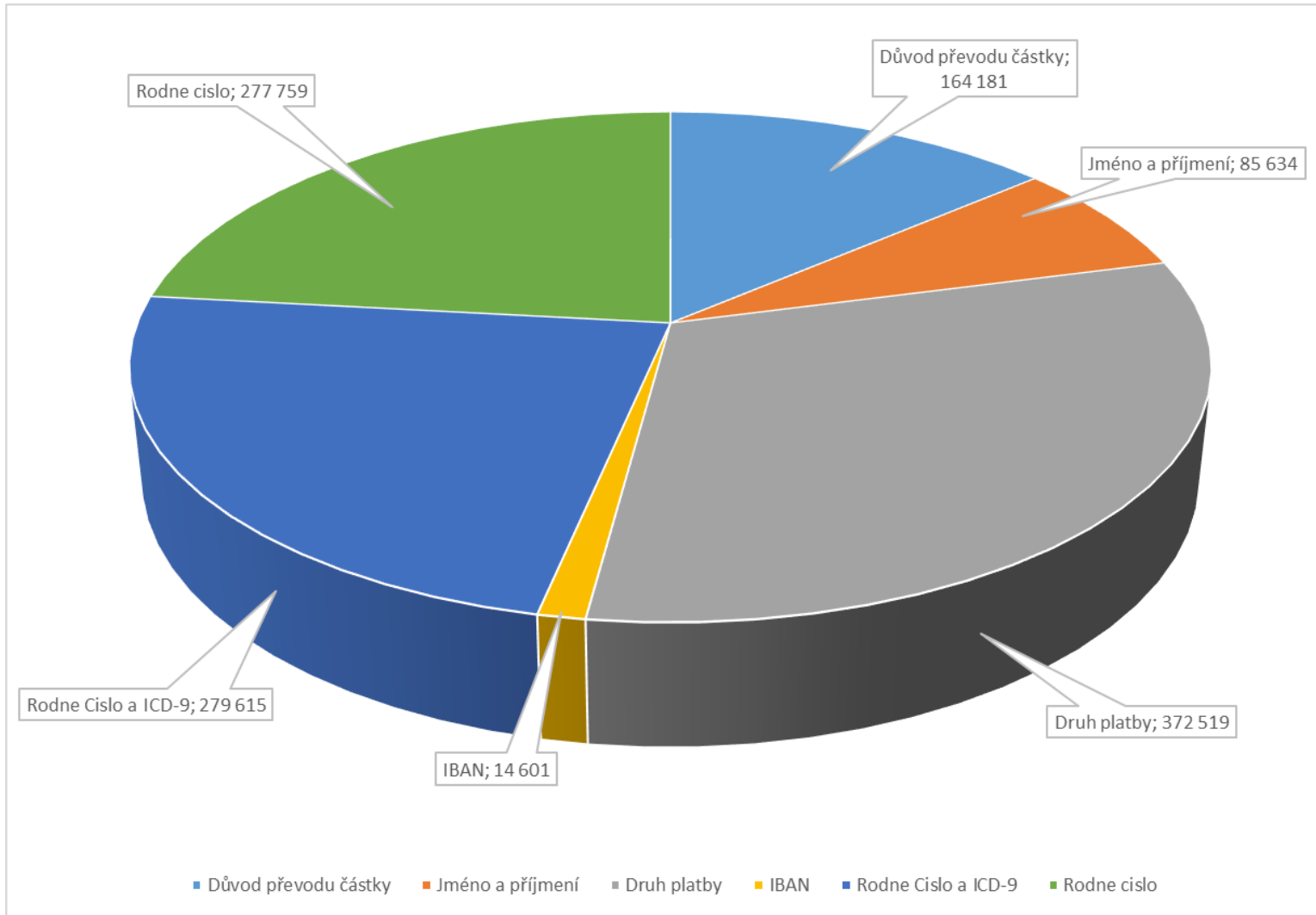
Zákazník z veřejné správy

Souborové úložiště

Celkem: 2 826 740 dokumentů

V 1 198 456 dokumentech byly detekovány 1 a více osobních údajů vč. citlivých osobních údajů

Čísla z praxe – jaké osobní údaje nacházíme



Zákazník z veřejné správy

Souborové úložiště

Celkem 18 550 425
dokumentů

V nich nalezeno celkem v
různých kombinacích
59 556 747 osobních a
citlivých osobních údajů

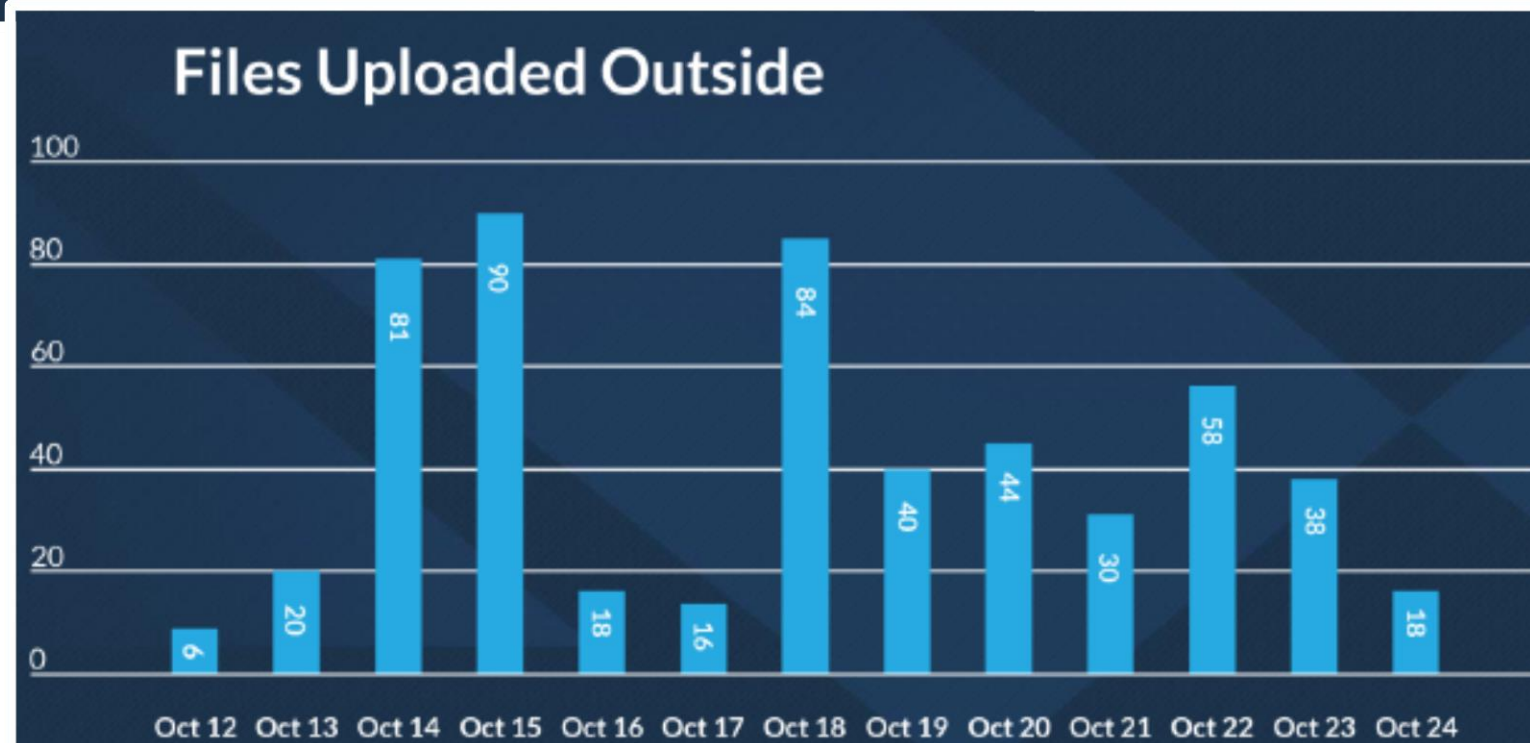
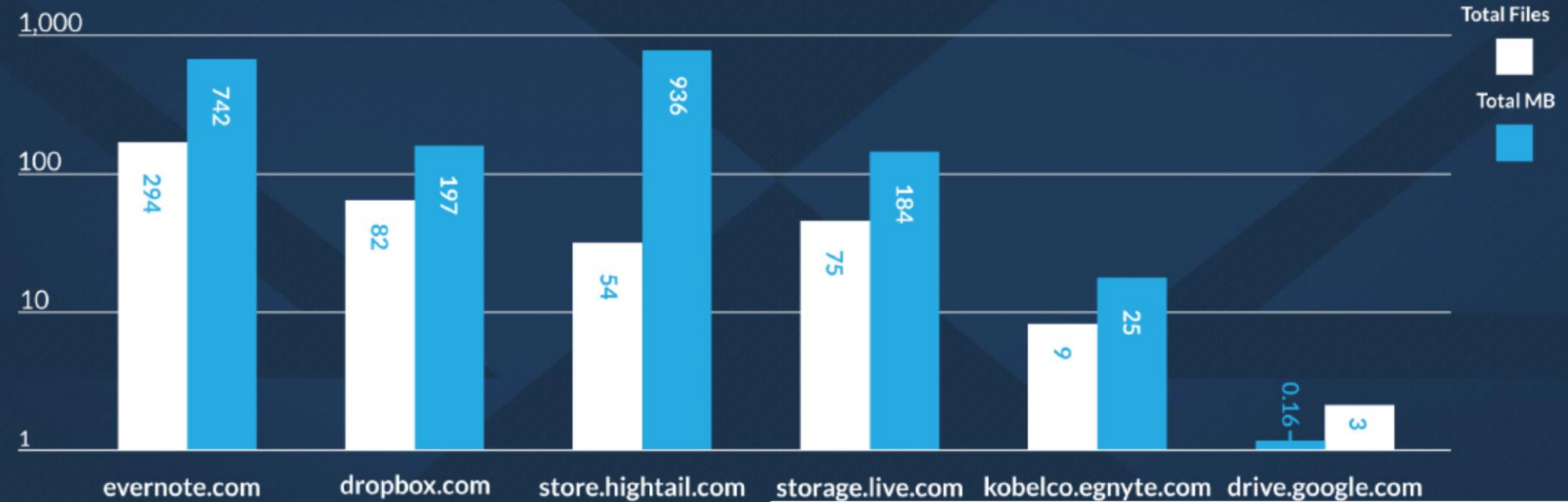
Fáze 2 - Analýza dat v pohybu

Zmapujte pohyb osobních dat

Tato analýza identifikuje jak se GDPR data pohybují uvnitř Vaší organizace a jakými cestami Vaši organizaci opouštějí. Naše platforma používá stejné datové vzory jako při analýze statických dat a to za účelem identifikace:

Všech typů osobních dat v pohybu

- Úrovně citlivostí těchto dat v pohybu
- Zdroj a cíl, tedy odkud a kam jsou osobní data přenášena
- Kanály, kterými osobní data opouštějí Vaši organizaci, např. web, email....



Fáze 3 - Report a doporučení

Připravte se na nápravná opatření

Jakmile jsou obě analýzy (statická data a data v pohybu) dokončeny, poskytne Vám Atos náhled na Vaše GDPR data který potřebujete k rozhodnutí, kde jsou rizika největší a jaké by měly být Vaše další kroky. Tento náhled ve formě reportu v sobě zahrnuje:

- Ucelený přehled rizik
- Detailní report analýzy dat
- Přehled zjištění
- Doporučení **strategie** nápravných opatření

4

Report a návrh nápravných
opatření

Fáze 3 - Report

Detailní popisy

Atos

Data of Interest Definition

Policies are an important aspect of the data exposure assessment. Policies determine the data patterns that are of interest and that are potentially sensitive. As well as 'out of the box' policies,

Atos

Introduction

This data exposure assessment report has been produced by Digital Guardian for <Customer Name> following the completion of the data analysis tasks performed on premise at <Customer Name> data centers located in <location> and <location>.

The report contains a detailed analysis of <Customer Name>'s storage capabilities using policies agreed with <Customer Name>. <Customer Name> identified a number of observations that they wished to be advised on if any incidents were generated during the assessment.

The data exposure assessment has provided visibility of sensitive data across multiple channels including Email, Web and storage repositories. During the assessment a number of "significant" violations have been cataloged to <Customer Name>. These incidents would pose a severe impact on the reputation of <Customer Name>, and possible financial bearing should they continue to occur.

Assessment Scope

«Customer Name» chose to monitor email and web traffic crossing the corporate boundary in «Location» and «Location». «Customer Name» also chose to send data repositories to identify the potential presence of sensitive data. Email and Web protection identification policies were configured to only monitor for traffic, and the system was configured to not store any file attachments contained in outbound email communications or web postings. Traffic was monitored for at 31 day period.

The discovery identification policies were configured to not store any artifacts relating to any identified files. All data repositories were scanned in a single pass.

Data Repositories

Detailed below are the data repositories that were identified by <Customer Name>

Network Share	\\sql2012.demoslab.local	(General Storage Repository)
SQL Server	demo-lab-my.sharepoint.com	(SQL Database Server)
OneDrive for Business		(Corporate OneDrive)

Network Communication Monitoring

Digital Guardian 98 LP email and web protection modules were enabled and activated. All outbound corporate email was monitored as part of the [assessment](#). The web protection module was integrated into <Our former Name> existing web security proxy [appliance](#). Squid item-0-0-0-0.com, which was identified as a squid proxy server.

En all Configuration

<Customer Name> uses both an on-premise email solution, Exchange 2013, and an Office 365 tenancy. Two email modules were installed, one to process inbound on-premise traffic and one to process outbound email originating from the cloud service. Once processed all outbound email was then delivered only to the corporate MTA, mailstore01b.com, for onward delivery to the intended recipient.

Web configuration

All Internet bound web traffic passes through a squid proxy server, squid.demolab.com. The squid proxy server was configured to direct all web posts to the Digital Guardian nDLP DAP service, where all posts were scanned. No blocking of posts was configured.

Proprietary and Confidential

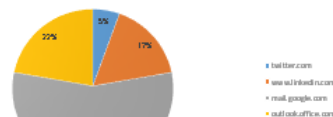
Datový audit

Atos

Top Policies by Protocol

Atos

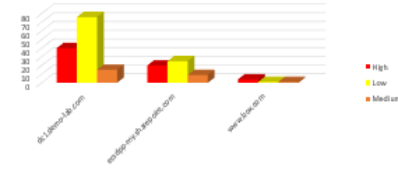
Web Incidents by Destination Web Host



Corporate data has been deleted within web transactions. Over 50% of all incidents were internal users sending data to gmail. This included PCI and PII data, which can result in large financial penalties.

Data at Risk Analysis: 46

Discovery Incident Severity Breakdown by Repository



The data stores can have identified ranges of incidents on all repositories scanned. Internal file shares have highly confidential information stored on them, as do the corporate One Drive for Business and Box accounts. The cloud data can potentially be shared with external parties and should be removed as soon as possible.

Proprietary and Confidential

Doporučení

AtoS

Conclusion And Recommendation

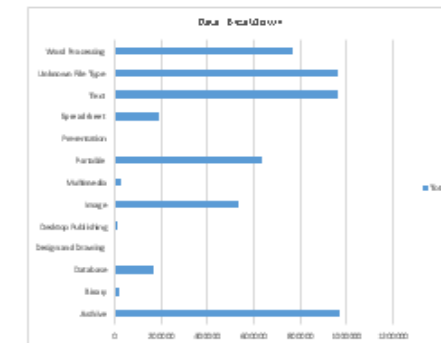
Atos

6 out of 7 G2E files contained data matching creek care patterns, of which a large proportion of these files contained more than 10 instances of creek care patterns. In the context of these files, it is reasonable by the accuracy angle, none of the data has been secured with either pass-ports protection or encryption, potentially exposing the contents to unauthorized access.

During policy accuracy validation tasks, the FBI's department shared files were limited to its certified highly confidential employee's intrusion. The FBI was not aware of other plans or encryption technologies, leaving the FBI unable to work on these cases. There were many

Digitized files clearly indicate the presence of a file record that is solely in a source repository, as opposed to a file record that is solely in a source repository. This policy was implemented to ensure the functionality of the Digital Data File (DDF) and registration technology, which can be used to produce a permanent record of a file record in a source repository.

Business Overview



Proprietary and Confidential

5 základních otázek – pamatujete?

Otázka	Výstup v reportu
1. Jaká osobní data občanů EU máte v držení?	Detailní popis, kde se data obsahující osobní údaje nacházejí vč. rozložení po jednotlivých zdrojích.
2. Jak citlivá data to jsou?	Popis způsobů vč. četnosti, jak osobní údaje opouštějí Vaši organizaci.
3. Kde přesně v rámci organizace se tato nacházejí?	Detailní popis úložišť obsahujících osobní data.
4. Jak se v rámci organizace pohybují a kam a jakými kanály z organizace odcházejí?	Real-time a historický pohled na osobní data opouštějící Vaši organizaci umožní detekovat a notifikovat o potenciálním úniku osobních dat.
5. Jak se s nimi pracuje a komu jsou poskytována?	Doporučení politik, architektury a životního cyklu dokumentů k zajištění vyšší úrovně ochrany.

5

Zavádění nápravných opatření

Management summary nápravných opatření

ID	Popis problému	Úroveň rizika	Opatrenia	Doba realizácie (týždne/Mesiace)	Náklady na implementáciu opatrenia (MD/ Eur bez DPH)	Ročné náklady na správu implementovaného opatrenia (MD / Eur bez DPH)	Priorita riešenia (1/2/3)*
ID6	Nie sú jasne identifikované všetky osobné údaje, informačné systémy osobných údajov, spracovateľské operácie s osobnými údajmi ani subjekty, ktoré sa podieľajú na spracúvaní osobných údajov.	Vysoká	A) Vykonať audit spracúvania osobných údajov. A) Identifikovať všetky spracovateľské operácie s osobnými údajmi. A) Identifikovať všetky systémy osobných údajov. A) Identifikovať všetkých sprostredkovateľov. A) Identifikovať všetkých zamestnancov prichádzajúcich do styku s osobnými údajmi.	1-2 Mes.	100 MD	20 MD	1
ID18	Na PCs, notebookoch a serveroch nie je kontrolované, ktoré údaje odchádzajú/prichádzajú z/na koncových zariadení.	Kritická	A) Zadefinovať citlivé dáta, ktoré majú byť chránené. B) Zaviesť pravidlá na ochranu pred únikom citlivých dát. C) Implementovať nástroje a bezpečnostné mechanizmy slúžiace na ochranu úniku citlivých a dôverných informácií prostredníctvom elektronickej pošty, internetu, FTP komunikácie a využitím USB, Bluetooth a pod. rozhraní – implementovať DLP (Data Leak Prevention systému).	1,5Mes – 4Mes.	50 MD SW/HW: 150-200 tis. Eur	50 MD	1

Technické a procesní specifikace coby podklad pro realizaci nápravných opatření

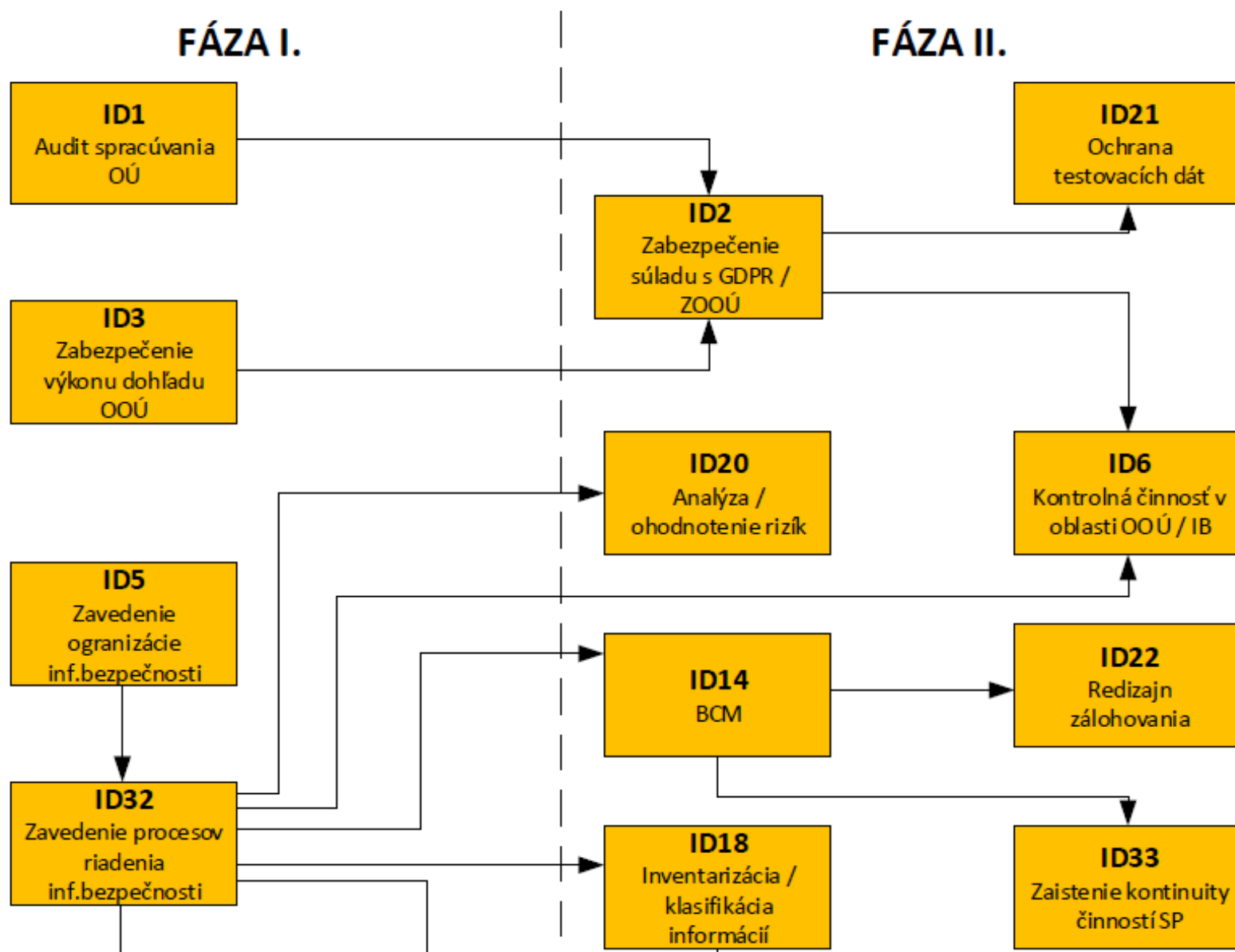
Technická špecifikácia:

Minimální požadavky na dodávané řešení jsou následující:



<u>Parameter</u>	<u>Minimálna požiadavka obstarávateľa</u>
<u>NetFlow Sonda</u>	
<u>Pasívne zapojenie</u>	<u>Pasívne zapojenie bez vplyvu na monitorovanie sieť (SPAN / mirror portami) pre každú lokalitu</u>
<u>Inštalácia</u>	HW, Racková montáž
<u>Management rozhranie</u>	2 x (administratívne) porty 10/100 / 1000Mb / s (UTP kabeláž) pre zabezpečenú vzdialenú správu a prenos NetFlow dát, zabezpečená vzdialená správa, dohľad a konfigurácia - SSH, HTTPS.
<u>Správa užívateľov a prístupových práv</u>	Správa užívateľov a prístupových práv na zariadení prostredníctvom užívateľských rolí.
<u>Nastaviteľná rýchlosť monitorovacej linky</u>	2x 10 Gb / s na optickom rozhraní (2x 10G-SFP-SR)
<u>Vstavaný kolektor</u>	Vstavaný kolektor pre dočasné ukladanie flow štatistík (zaistenie redundancie) min o kapacite 0,5 TB
<u>Časová synchronizácia</u>	Časová synchronizácia zariadenia proti centrálnemu zdroju času na sieti.

Roadmap nápravných opatření



Součástí reportu je i kvantifikace nápravných opatření a návrh jejich rozložení v čase podle časových, finančních možností zákazníka.

— ATOS program ochrany GDPR dat

Vyhodnocení
rizik GDPR dat

Poznejte, kde máte uložena osobní data, jak je s nimi nakládáno, která data jsou ta nejcitlivější a požadujete pro ně vyšší ochranu.

Automatizace
klasifikace
všech osobních
dat

Zautomatizujte klasifikaci Vašich osobních dat s důrazem na zdroje a jejich kontrolu

Zabezpečení
ochrany dat

Používejte technologie jako je DLP, Identity Access Management a šifrování

Úprava
plánu zvládní
incidentů

Zaktualizujte si své plány zvládní detekovaných incidentů abyste byli na podobné situace připraveni

Demontrace
souladu s
GDPR

Použijte své analýzy a jejich výstupy k předvedení svého souladu s požadavky GDPR

Atos

Trusted partner for your Digital Journey