Co se děje v IT

aneb krátké zamyšlení nad výzvami (příležitostmi) nové doby

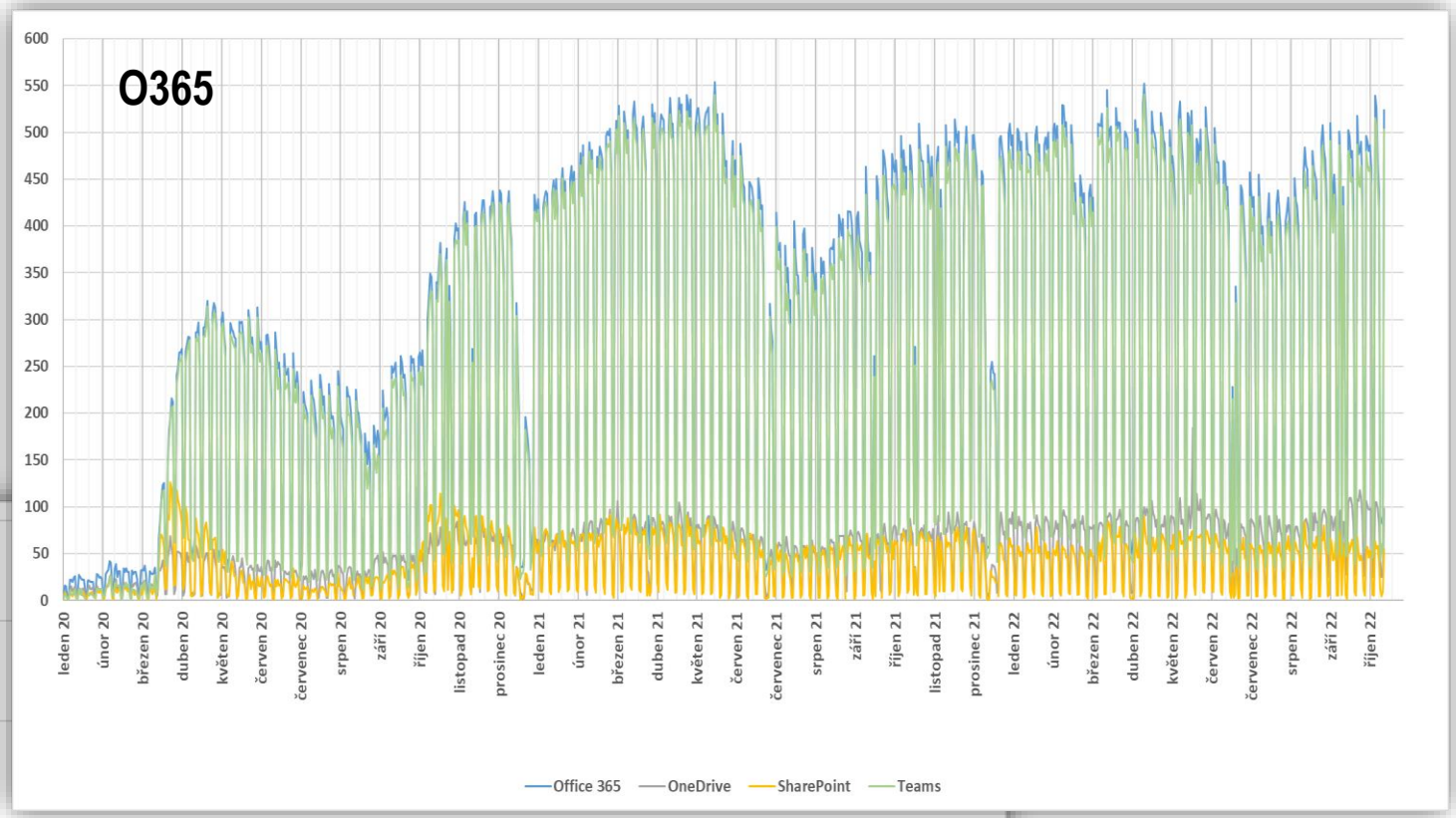
CACIO 22.11.2022

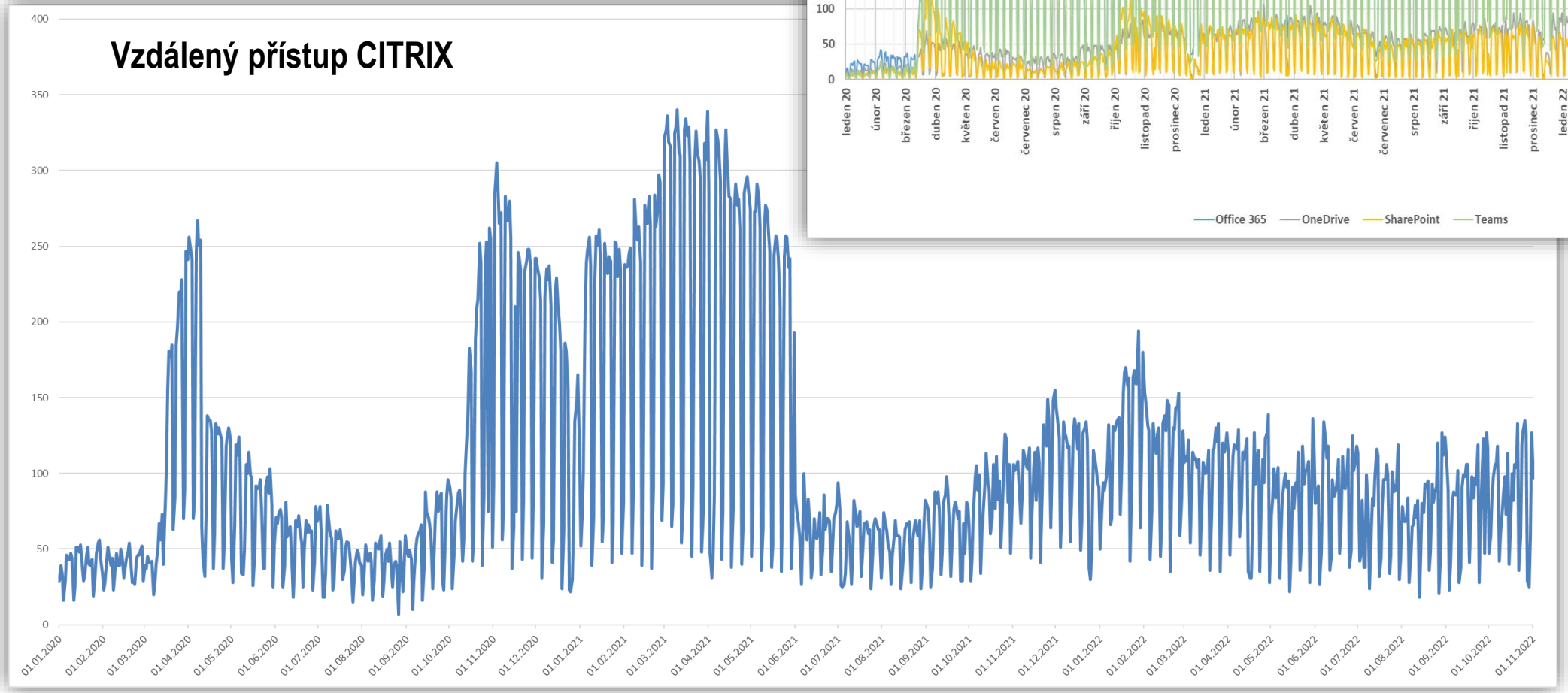
Miroslav Hubner

- Covid
- DPI
- DPH
- Energetický zákon
- Energetické společenství
- Fotovoltaiky
- Elektromoblita
- Úsporný tarif
- Kampaně
- Prémie
- Zastropování cen
- Síťové semafory
- Změny v řízení sítí
- Black out opatření, záložní pracoviště

Vzdálená práce

- Standard zasedačky
- Standard stanice
- Smart stanice
- Záložní pracoviště





Krizové řízení

Proč bylo zavedeno Krizové řízení (výchozí situace)

- **Více kritických projektů** (převážně legislativních), které se musejí realizovat **v krátkém čase**
- **Přímý dopad projektů na vedení** společnosti PRE
- **Nejasné zadání** u některých kritických projektů
- **Omezený počet osob** na straně IT a ostatních ovlivněných sekcí
- **Omezení systému** (technologické i funkční)
- Projekty jsou napříč skupinou PRE
- **Provázanost** jednotlivých kritických projektů (lidi, systémy)
- Principy a postupy standardního **liniového/projektového řízení nešlo aplikovat**

Vybrané projekty zařazené do Krizového řízení

> Úsporný tarif, DPI, EHP, Sdílení elektřiny v bytových domech, AMM centrála, Kampaně

Krizové řízení

> Postup a zásady

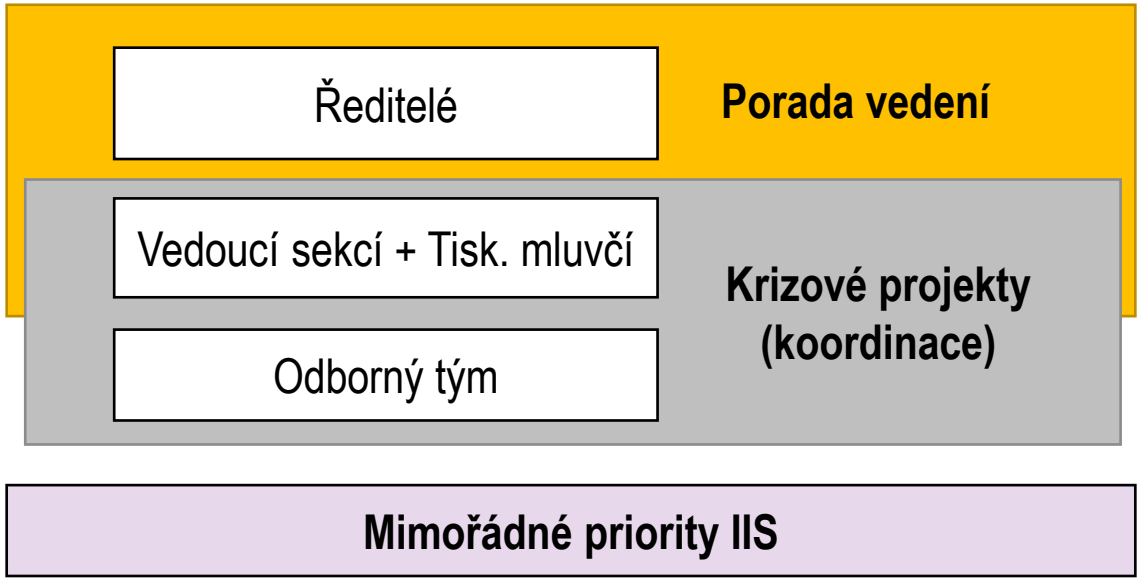
- > Vytvořena řídící / komunikační platforma, na které se průběžně komunikuje stav projektů a schvalují se změny
- > Vytvořen rámcový harmonogram a tým
- > Bližší zapojení ředitelů do projektů

- > Centralizované řízení
- > Jednotný cíl pro všechny sekce
- > Tvorba kompromisů v řešení
- > Rychlost realizace na úkor kvality
- > Průběžné informování

- > Omezení realizace nekritických projektů
- > Omezení dokumentace při realizaci projektů

- > **Trvání krizového řízení:** časově omezené

> Organizace



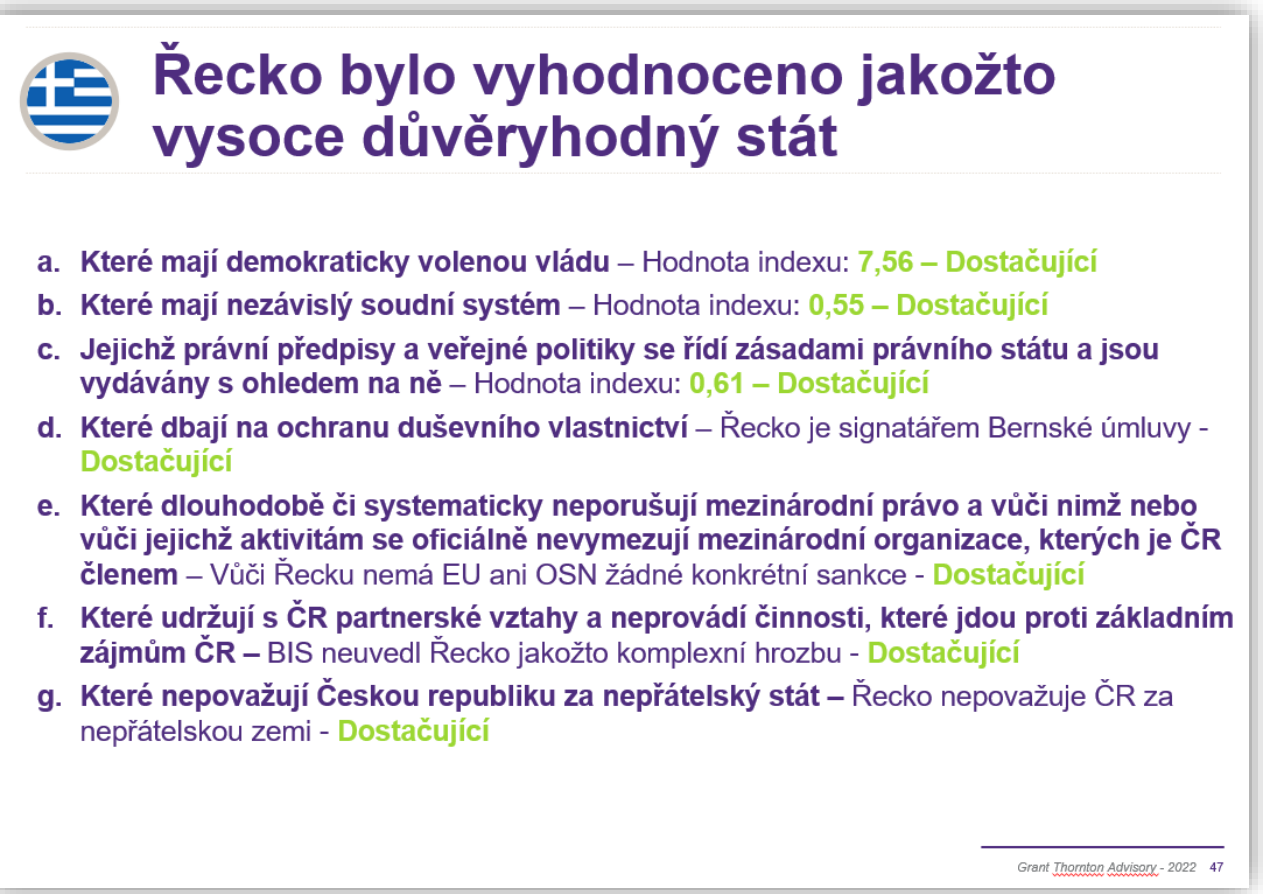
> Přínosy

- > Rychlost rozhodování
- > Rychlost realizace
- > Snížení realizace nepodstatných věcí
- > Informovanost napříč PRE

Řízení dodavatelů

Hodnotíme

> závislost
> důležitost
> spokojenost
> obrat
> růst
> Riziko (geopolitická vhodnost)



Kategorie	Hrozba
Vysoce důvěryhodné státy	Nízká
Důvěryhodné státy	Střední
Přijatelné státy	Vysoká
Nedůvěryhodné státy	**Kritická**

Bezpečnost

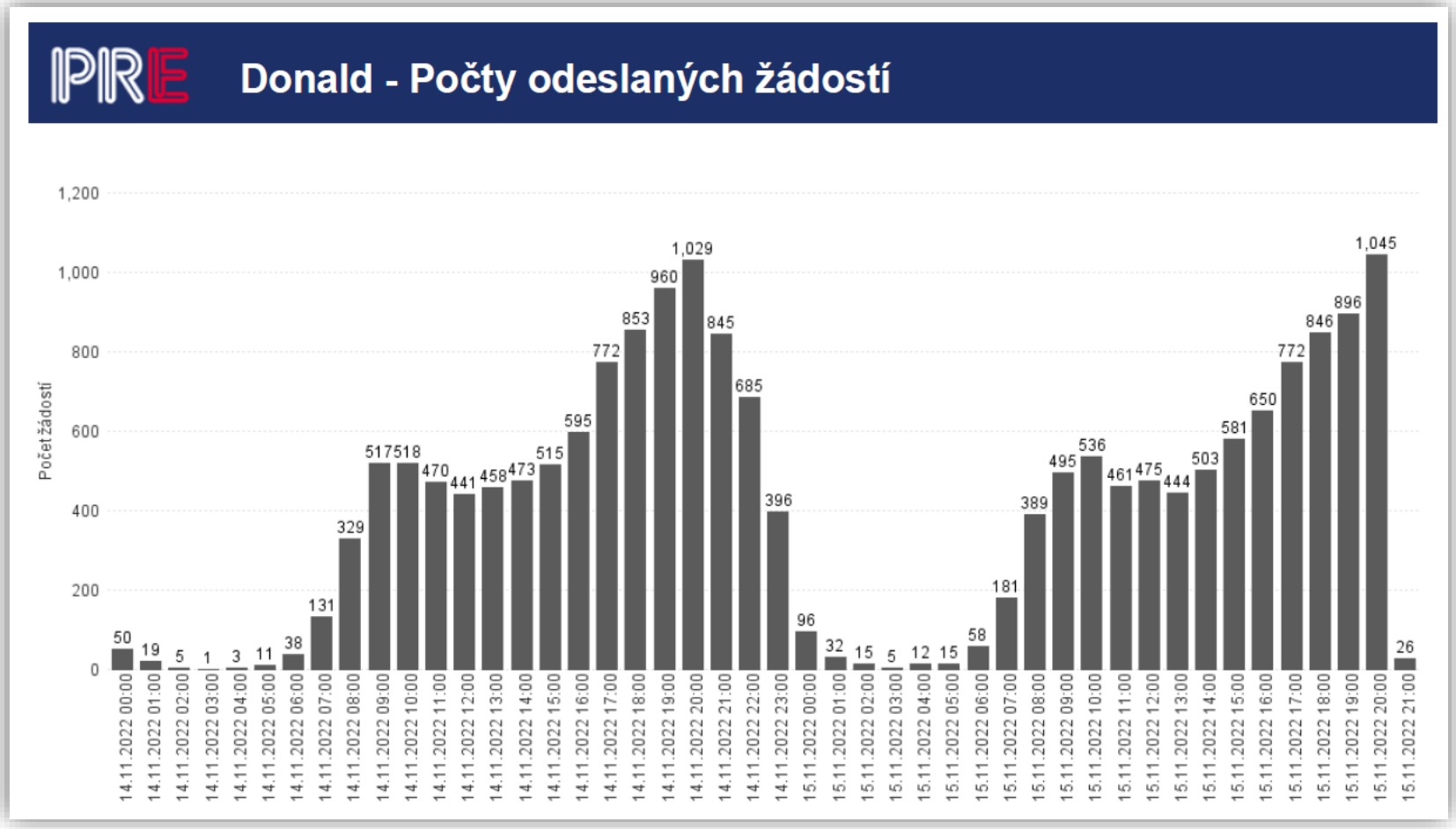
Stavy kybernetické bezpečnosti

- Obvyklé kybernetické nebezpečí
- Zvýšené kybernetické nebezpečí
- Kybernetické ohrožení (havárie)
- Kybernetická krize

Digitalizace procesů

	Typ podpisu	Důvěryhodnost podpisu	Výhody	Nevýhody
A	**Prostý elektronický podpis** • Podpis jako prostý text či obrázek • Zaškrtávací pole • Kliknutí na tlačítko	NÍZKÁ	• Jednoduché SW řešení • Uživatelům není nutné nic vystavovat ani obnovovat • Bez externích nákladů • Možnost hromadného podepisování většího množství dokumentů	• Není právně srovnatelné s vlastnoručním podpisem na papír – vhodné pouze pro vybrané dokumenty
B	**Prostý el. podpis + kvalifikovaná el. pečeť organizace** • Autentifikace uživatele např. přihlášením přes AD • Prostý el. podpis je na dokument přidán skrze el. pečeť	NÍZKÁ/STŘEDNÍ	• Jednoduché SW řešení • Stačí 1 pečeť na společnost • Uživatelům není nutné vystavovat/obnovovat certifikát + bez nákladů na čtečku a kartu	• Nižší „váha“ podpisu, než kvalifikovaný el. podpis • Nutnost použití kvalifikované elektronické pečetě (elektronický podpis za organizaci)
C	**Zaručený elektronický podpis** • Certifikát od interní certifikační autority (na kartě / bezpečně uloženo v KeyStore na PC)	STŘEDNÍ	• Vystavení certifikátu je řešeno plně interně – bez nákladů na externí autoritu • Možnost hromadného podepisování většího množství dokumentů	• Nutnost pravidelné obnovy (1x ročně) • Vystavení a obnovu je nutné provádět pro každého uživatele zvlášť – provádí interně PRE • Každý uživatel musí být vybaven kartou/tokenem s certifikátem a čtečkou
D	**Kvalifikovaný el. podpis** • Kvalifikovaný certifikát od externí autority (na kartě / fyzickém nosiči)	VYSOKÁ	• Právně srovnatelný s vlastnoručním podpisem na papír • Možnost hromadného podepisování většího množství dokumentů	• Nutnost pravidelné obnovy (1x ročně) • Vystavení/obnova pro každého uživatele zvlášť – provádí pracovník autority • Vystavení a obnova je zpoplatněna • Každý uživatel musí být vybaven kartou/tokenem s certifikátem a čtečkou
E	**Biometrický podpis** • Vlastnoruční elektronický podpis na podpisovém padu	VYSOKÁ	• Právně srovnatelný s vlastnoručním podpisem na papír	• Problematické ověření podepisujícího • Přísné podmínky pro zpracování osobních údajů • Všichni uživatelé musí mít přístup k podpis. padu • Nelze hromadně podepisovat větší množství dokumentů

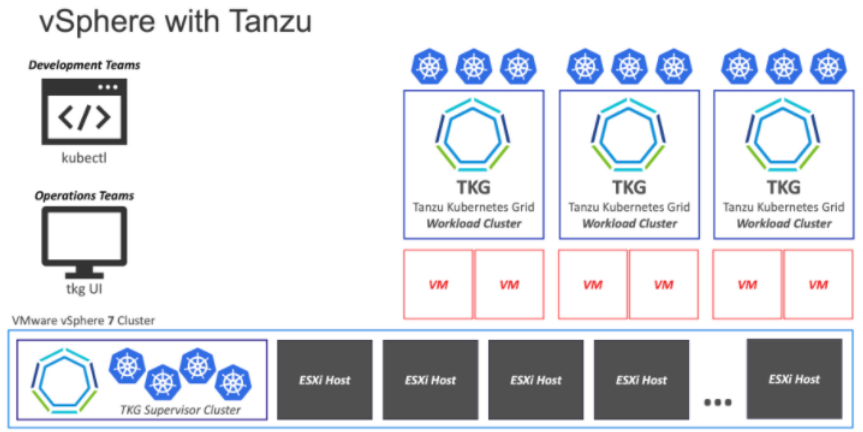
Ukázka kampaně



- Rychlý vývoj
- Výkonový test (14 dní ladění)
- Poplach při 15 000 kontaktů/hod (design 30 000 kontaktů/hodinu)
- Technická pohotovost 24 x 7

Kontejnerizace

- **Izolace**
  - Každá aplikace má u sebe své prostředí, ve kterém běží
  - Toto prostředí není ovlivněno jinými aplikacemi, nebo činnostmi, nebo serverem, na kterém aplikace běží
  - Aplikaci lze upgradovat samostatně bez dopadu na okolí
  - Aplikaci není potřeba upgradovat při upgradu serveru, na kterém běží
- Naprosto totožné prostředí na vývoji, testu a produkci – **prostředí je součástí aplikace**



- Výrazně jednodušší deployment a správa různých verzí aplikace
- **Vysoká dostupnost** – v případě výpadku jednoho serveru platformy nebo jeho odstávky je aplikace stále dostupná
- **Škálovatelnost** - možno jednoduše spustit více instancí aplikace (pokud to aplikace umožňuje)
- **Optimální využití HW** - prostředky jsou aplikacemi sdíleny a přidělovány dle potřeb aplikace
- Častější, jednodušší a bez problémovější releasy
- Řádově méně problémů při nasazování a údržbě aplikace

- **Dva hlavní hráči na trhu – VMware TKG a OpenShift**
  - Prakticky stejná funkcionalita – Kunernetes s funkcemi navíc
  - Relativně obdobná cena
- Čistý Kubernetes bez podpory - ne

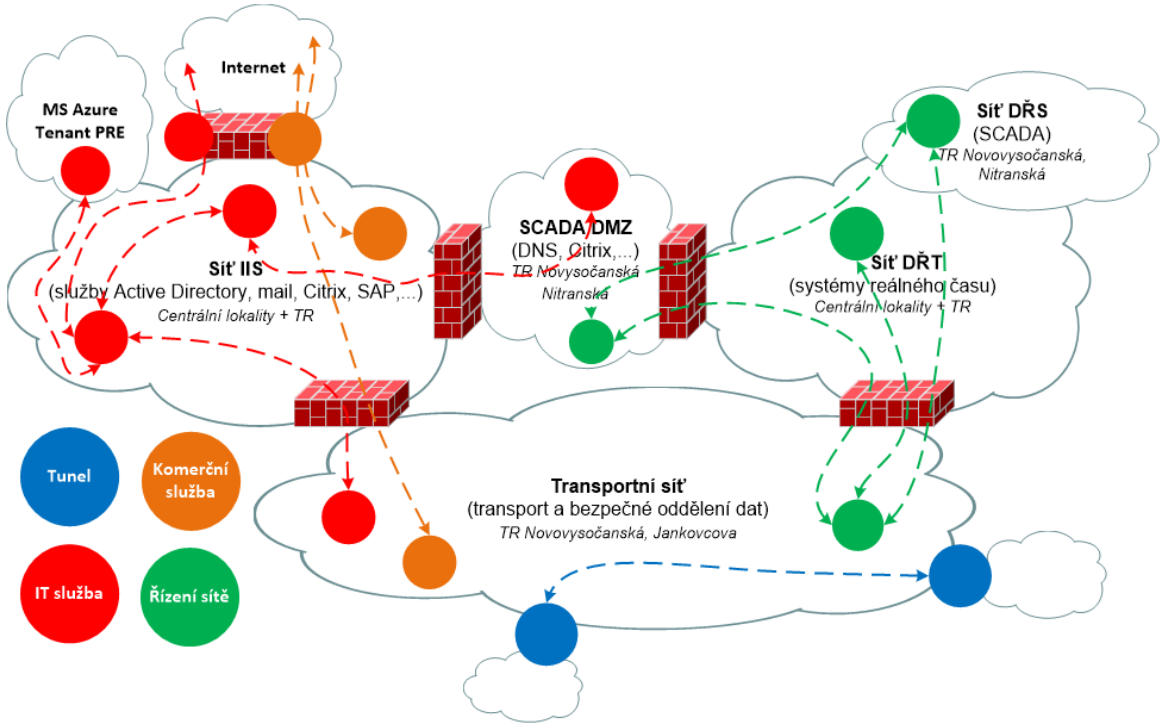
- Obecné doporučení je, tam kde je již použit VMware vyplatí se spíše TKG platforma – synergické efekty jak v ceně tak v technologiích
  - VMware máme a chceme s ním pokračovat
  - Vypadá to, že některé funkce, které TKG poskytuje by do budoucna mohly být zdarma v licencích, které potřebujeme i bez TKG
- Personální zajištění
  - Naše zdroje – G 34 430 (Mařík), G 34 300 (Kyndl) + aplikační správci
  - ITS
  - ICZ
- Zdvojení veškerých provozních úkonů (např. upgrade platformy, provozní problémy)
- **Dlouhodobá strategie**

  Vzhledem využívání dalších produktů VMware je pro nás i z dlouhodobého hlediska výhodnější orientace na TKG. Jak z provozních, tak finančních důvodů.

  Pokud se zásadním způsobem nezmění podmínky trhu, provozu nebo kvality platformy, měli bychom se této strategie držet.

Jak mění nová doba řízení IT

> Cloudové služby, příležitosti i hrozby
> Kontejnerizace
> Změna rozsahu služeb na 24x7
> Generační rozvoj datové sítě
> Nákup služeb



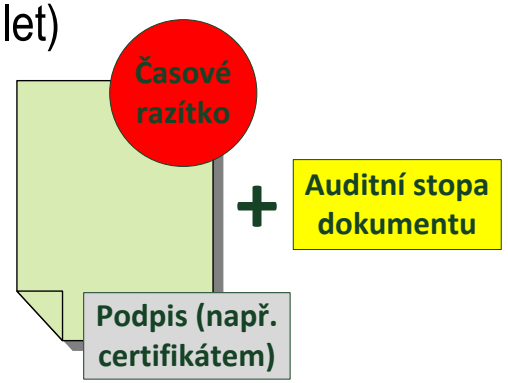
PRE

Elektronické podepisování - základní pojmy

Elektronický podpis	Fyzická osoba – jednotlivec	Právnická osoba – Organizace
Bez certifikátu – prostý	**Prostý elektronický podpis** • Prostý text, obrázek podpisu, potvrzení akcí, apod.	---
Založený na certifikátu	**Zaručený / Kvalifikovaný elektronický podpis** • **Ověření totožnosti podepsané osoby** • **Ověření, zda nebyl dokument změněn** • Důvěryhodnost podle certifikační autority (interní / kvalifikovaná externí) • Platnost certifikátu 1 rok – nutnost obnovovat (u kvalifikovaného zpoplatněno)	**Elektronická pečeť** • **Ověření organizace** • **Ověření, zda nebyl dokument změněn** • Důvěryhodnost podle certifikační autority (interní / kvalifikovaná externí) • Platnost certifikátu 1 rok – nutnost obnovovat (u kvalifikovaného zpoplatněno)
Biometrický podpis	**Dynamický biometrický podpis** • Podpisový pad – záznam křivky podpisu, tlaku, sklonu pera	---

> Časové razítko

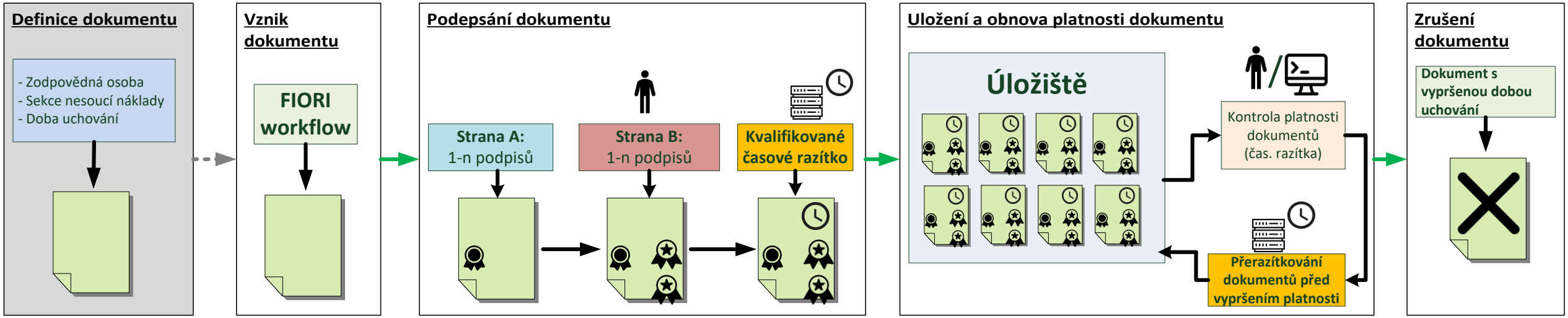
- ***Garance času podpisu*** + ***prodloužení platnosti*** elektronického podpisu certifikátem (na 5 let)
- Vystavuje kvalifikovaná autorita (PostSignum, I.CA) – 1-2 Kč za kus



> Archivace podepsaných dokumentů

- Dlouhodobé uchování v logickém archivu
  - Uchování dokumentu a auditní stopy (log/historie dokumentu) a udržení platnosti

Životní cyklus dokumentu

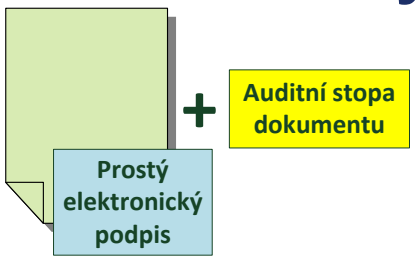


- **Definice dokumentu**
  - Při vytváření životního cyklu daného dokumentu
- **Vznik dokumentu**
  - Vznik konkrétního dokumentu (workflow/formulář ve FIORI)
- **Podepsání dokumentu**
  - Samostatné FIORI workflow + podepisování skrze podepisovací komponentu Obelisk
- **Uložení a uchování platnosti dokumentu**
  - Pravidelné přerazítkování
- **Zrušení dokumentu** – po vypršení doby uchování

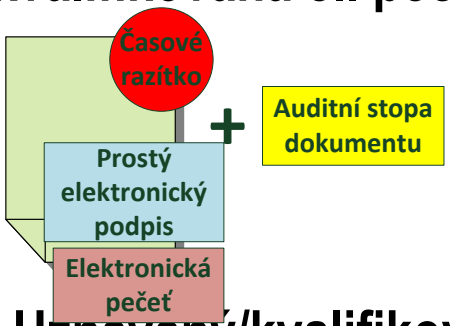
Podepsání dokumentu – typy el. podpisů

> A) Prostý elektronický podpis

- prostý text či obrázek

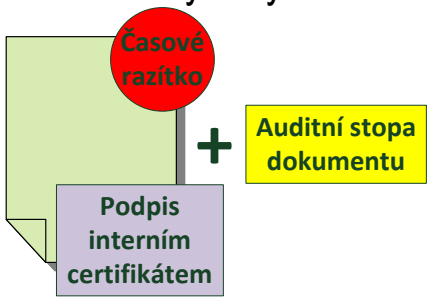


> B) Prostý el. podpis přihlášeného uživatele + kvalifikovaná el. pečeť organizace



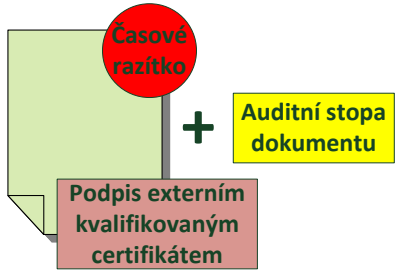
> C) Zaručený elektronický podpis

> Certifikát vydaný interní certifikační autoritou PRE



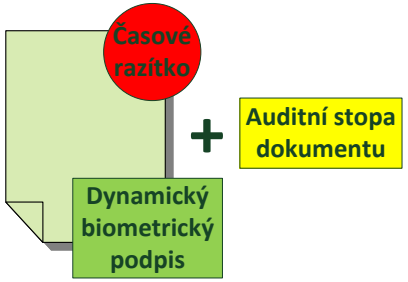
> D) Uznávaný/kvalifikovaný elektronický podpis

- Kvalifikovaný certifikát od externí autority (PostSignum, I. CA)
- Uznávaný podpis = certifikát na libovolné kartě či jiném fyzickém tokenu
- Kvalifikovaný podpis = certifikát na kvalifikovaném médiu (vybrané karty a tokeny)



> E) biometrický podpis

- Vlastnoruční elektronický podpis na podpisovém padu

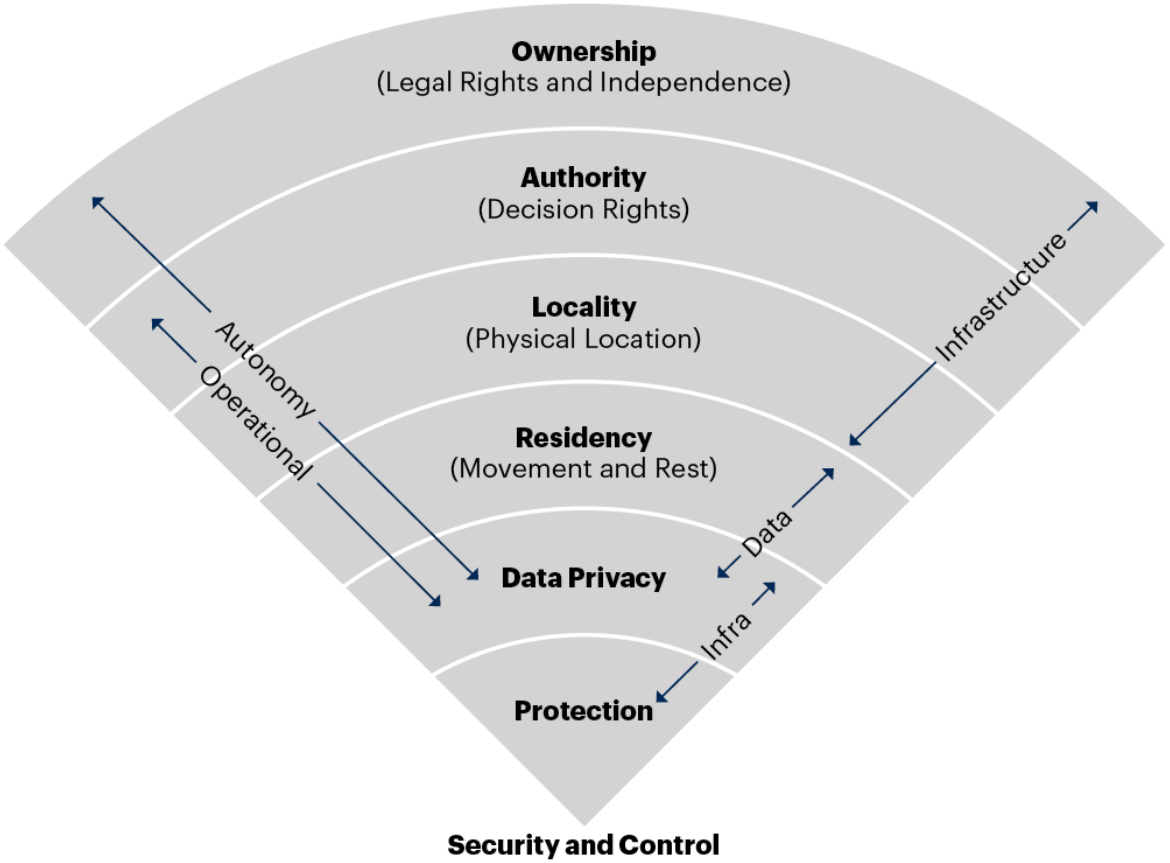


Cloudové služby dedikované regulovanému sektoru

> „Suverénní“ cloud
  - Cloudové služby poskytované v rámci 1 geografické oblasti
  - Splnění požadavků na umístění dat
  - Splnění místních legislativních požadavků

> Umožnění nezávislosti na zahraniční infrastruktuře
  - Ochrana před cizími zásahy
  - Zamezení přístupu cizích vlád

> Dedikované vládním a kritickým řešením



Source: Gartner
769931_C

Posun od Globálních k hybridním a případně lokálním řešením

Current Sovereign Cloud Approaches

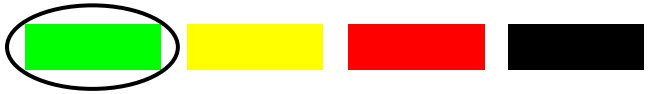
GLOBAL: Global Cloud Service Provider	GLOCAL: Global Cloud Service Provider With Domestic Partner	LOCAL: Domestic Cloud Service Provider
Base Safeguards:	**Base Safeguards:**	**Base Safeguards:**
Global cloud offerings, such as those featured in Magic Quadrant for Cloud Infrastructure and Platform Services, delivered from in-country or in-region data centres with standard security controls.	Provider enables **domestic partner or independent third party to provide oversight/monitoring** to ensure sovereignty is upheld.	**Domestic provider offering cloud service** using open source or other cloud software **that can be used perpetually.**
Advanced Safeguards:	**Advanced Safeguards:**	**Advanced Safeguards:**
Provider adds technologies that shield customer information from the provider*, e,.g., hold your own key (HYOK), privacy-enhancing compute (PEC), confidential computing, and autonomous distributed cloud.	**Domestic partner runs a separate copy** of the global cloud service. The domestic partner has full operational control using the software of the global cloud provider. Offering may exist next to (and compete with) the global providers own offerings in the country.	**Private (single-tenant) or on-premises instance** of above cloud service dedicated to one customer.
For Whom:	**For Whom:**	**For Whom:**
For organizations looking to fully leverage public cloud services and, where possible, addressing specific sovereignty through sovereignty-enhancing technologies.	For organizations that need assurance from a domestic organisation that the provided service is compliant with their requirements and/or that are required to have the service be fully provided by a domestic provider.	For regulated, critical and sensitive workloads and infrastructure where other options are not deemed acceptable by the local regulator, or where continuity of operations without dependence on foreign providers is required.

Lower ←	expected sovereignty level	→ Higher
Lower ←	expected resilience level	→ Higher
Lower ←	expected cost level	→ Higher
Higher ←	expected functionality level	→ Lower
Higher ←	expected scalability level	→ Lower
Higher ←	expected reliability level	→ Lower

Source: Gartner

769931_C

Stav: Obvyklé kybernetické nebezpečí



Rutinní stav

> dodržují se normy a pravidla

> běžný pohotovostní režim (PN PA 901)

> řešeny vesměs jednotlivé bezpečnostní události a incidenty, případně eskalace na základě závažnosti incidentu či jejich kumulace/souběhu

> **Preventivní organizační opatření**, mj.

- pravidla reakce na incidenty a stavy kyb. bezp.
- určení odpovědných rolí a kontakty na ně
- adresy a kontakty mimo organizaci
- vzory komunikace
- řízení rizik a zranitelností, kontroly a audity
- vzdělávání a osvěta uživatelů

Preventivní technická opatření, mj.

> ochrana perimetru (firewally, IDS /IPS, …)

> segmentace sítě

> antivirová ochrana, EDR, sandbox

> kontrola & filtrace IoC (indikátorů kompromitace)

> antispam, antimalware, …

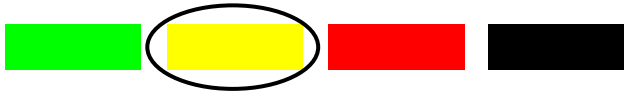
> dohledové a monitorovací systémy

> zálohování a archivace

> vzdálená správa PC

> patchování

Stav: Zvýšené kybernetické nebezpečí



Vyhlášení

> pokud se jedná o **dlouhodobé a mimořádné hrozící kybernetické nebezpečí**

> **vyhlašuje CIO** ve spolupráci s CISO

> informováno vedení IIS (6IIS), VS S 22 a S 28 & MKB ICS

> **určí se bezpečnostní štáb (IIS a ICS)**

> **rozhoduje/í VS v rámci působnosti, koordinuje CISO**

Průběh

> pravidelné hodnocení aktuálních rizik, stavu bezpečn. událostí a incidentů (zpravidla týdně)

> prioritní úsilí & investice do monitoringu, detekce a případných reakčních opatření i na úkor byznys projektů

> prioritní je ochrana perimetru, IT správce v případě incidentu nejprve zasahuje, až poté informuje

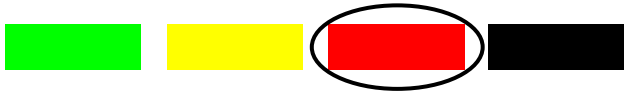
> CIO a CISO je okamžitě informován o všech provozních anomáliích

> kontrola či rozšíření preventivních opatření

> kontrola záložních pracovišť (BCP)

> v případě potřeby informování uživatelů o hrozícím nebezpečí a konkrétních rizicích

Stav: Kybernetické ohrožení / havárie



Vyhlášení

> pokud se jedná o **částečné či lokální omezení funkčnosti IT** vlivem kybernetického incidentu / útoku

> **vyhlašuje CIO** ve spolupráci s CISO

> informováno vedení IIS (6IIS), VS S 22 a S 28 & MKB ICS a vedení dotčených byznys sekcí

> **určí se havarijní štáb (IIS a ICS + dotčený byznys)**

> **rozhoduje/í VS v rámci působnosti, koordinuje CISO**

> VS ve spolupráci s CISO má právo rozšířit pohotovost či nařídit mimořádné práce

Průběh

> prioritní při odstraňování incidentu:
- zamezení útoku, odstranění příčiny incidentu
- obnovení dat & funkčnosti
- sběr forenzních důkazů

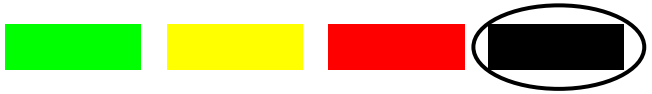
> **priority obnovy systémů:**
- obnova nezbytné infrastruktury
- zajištění distribuce elektřiny
- trading
- komunikace se zákazníky
- kancelářské systémy, …

> informuje se PR, compliance, DPO, právní, HR

> rozhoduje se o informování úřadů a Policie

> rozhoduje se o informování zákazníků / veřejnosti

Stav: Kybernetická krize



Vyhlášení

> **pokud se jedná o plošné omezení funkčnosti IT vlivem kybernetického incidentu / útoku**
> **vyhlašuje GŘ** na základě odůvodněné žádosti CIO nebo CISO
> informováno vedení Skupiny PRE
> určí se **krizový štáb**
> **rozhoduje/í Ř a VS v rámci působnosti, koordinuje CISO**
> VS ve spolupráci s CISO má právo rozšířit pohotovost či nařídit mimořádné práce

Průběh

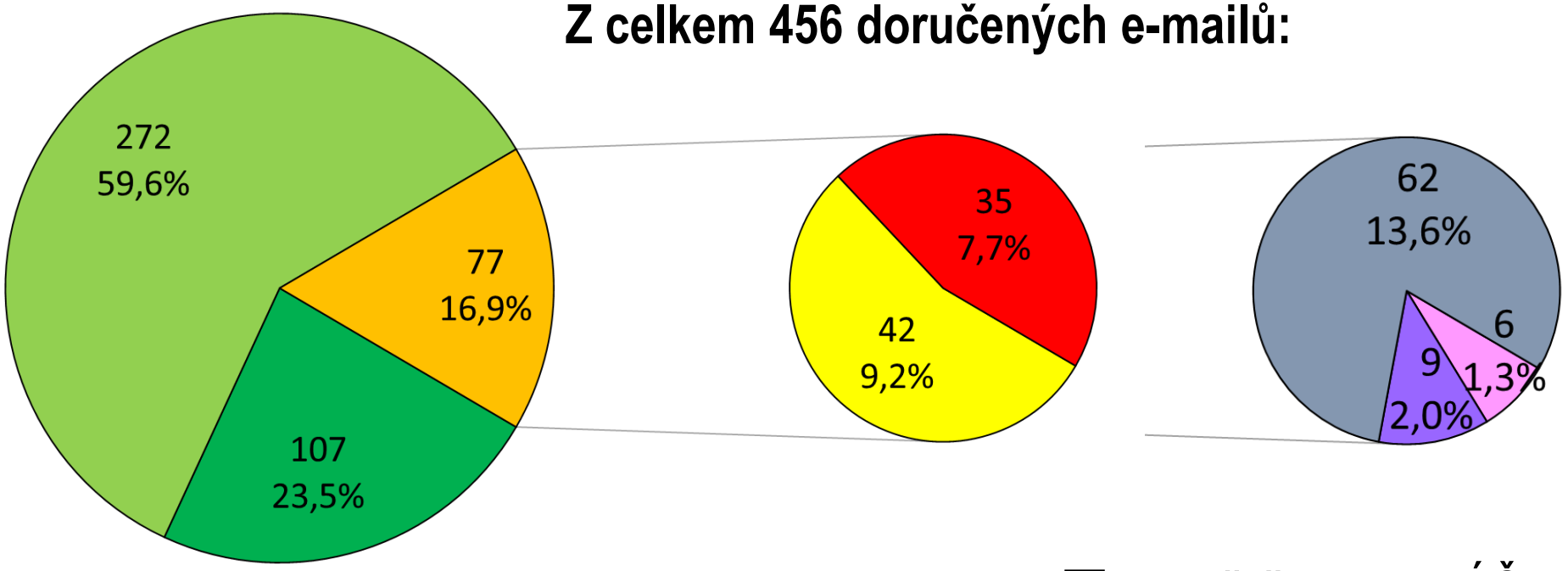
> prioritní řešení incidentu (až do zotavení)
> zajištění (náhradní) kontinuity byznysu
> defaultní vzdálený přístup dodavatelů zakázán, resp. jen na povolení
> rozhoduje se o informování úřadů
> rozhoduje se o informování zákazníků / veřejnosti

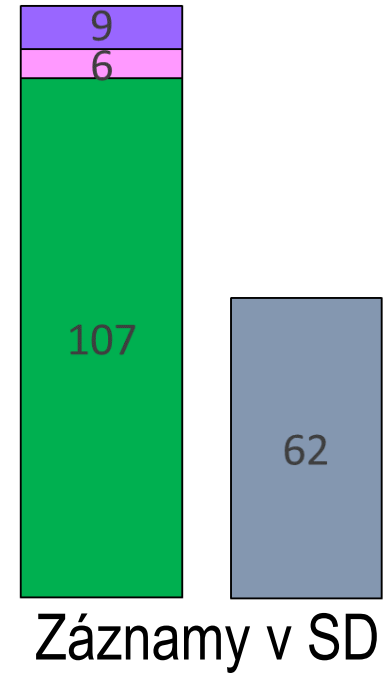
Ukončení

> rozhodnutím vedení společnosti
> CISO sepisuje závěrečnou zprávu, kterou schvaluje vedení společnosti

Celkové výsledky phishingových testů 6/2022

Z celkem 456 doručených e-mailů:

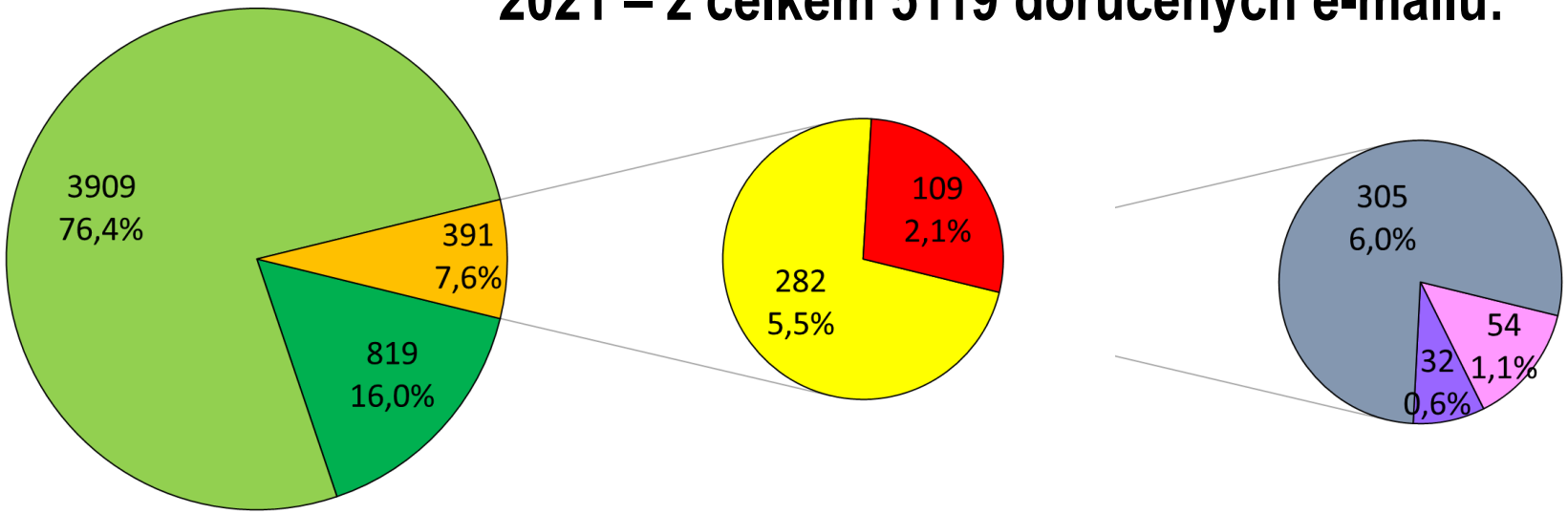


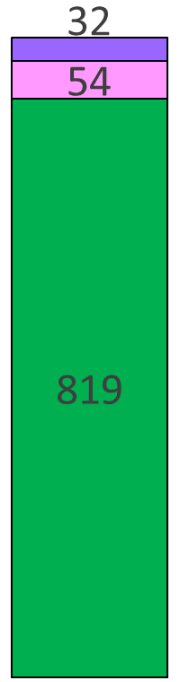


- Bez škodlivé interakce a NAHLÁŠENO
- Bez škodlivé interakce, ale NENAHLÁŠENO
- Minimálně 1. stupeň prohřešku (rozkliknutí odkazu nebo otevření přílohy)
- Jen 1. stupeň prohřešku (rozkliknutí odkazu nebo otevření přílohy)
- 1. a 2. stupeň prohřešku (zadání přihlašovacích údajů nebo povolení maker)
- Prohřešek NAHLÁŠEN
- Prohřešek NEPŘIZNÁN, nahlášeno podezření
- Prohřešek NENAHLÁŠEN

Celkové výsledky phishingových testů 2021 / 2022

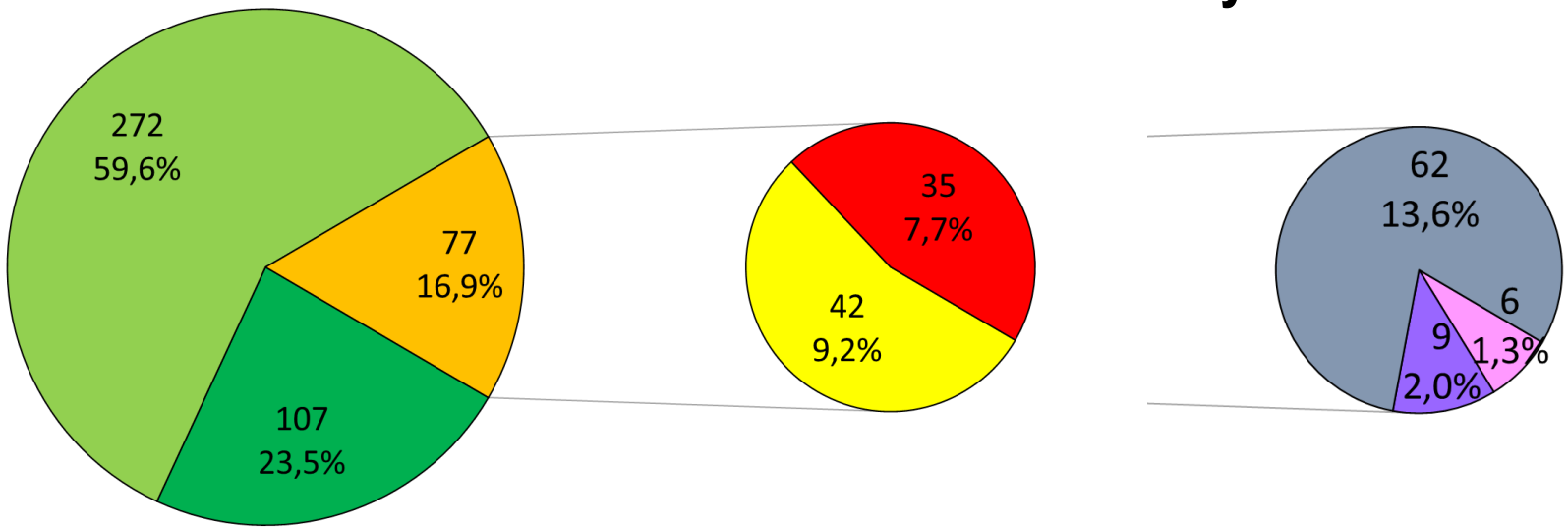
2021 – z celkem 5119 doručených e-mailů:

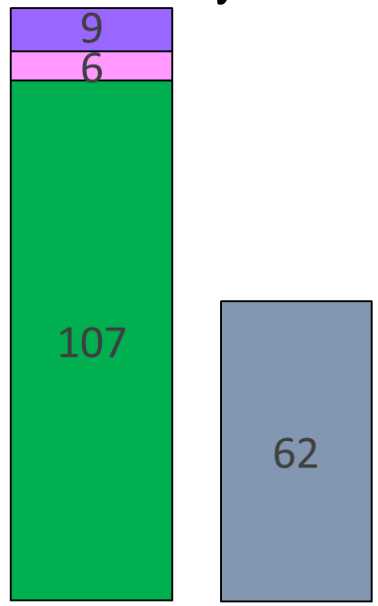




Záznamy v SD

2022 – z celkem 456 doručených e-mailů:

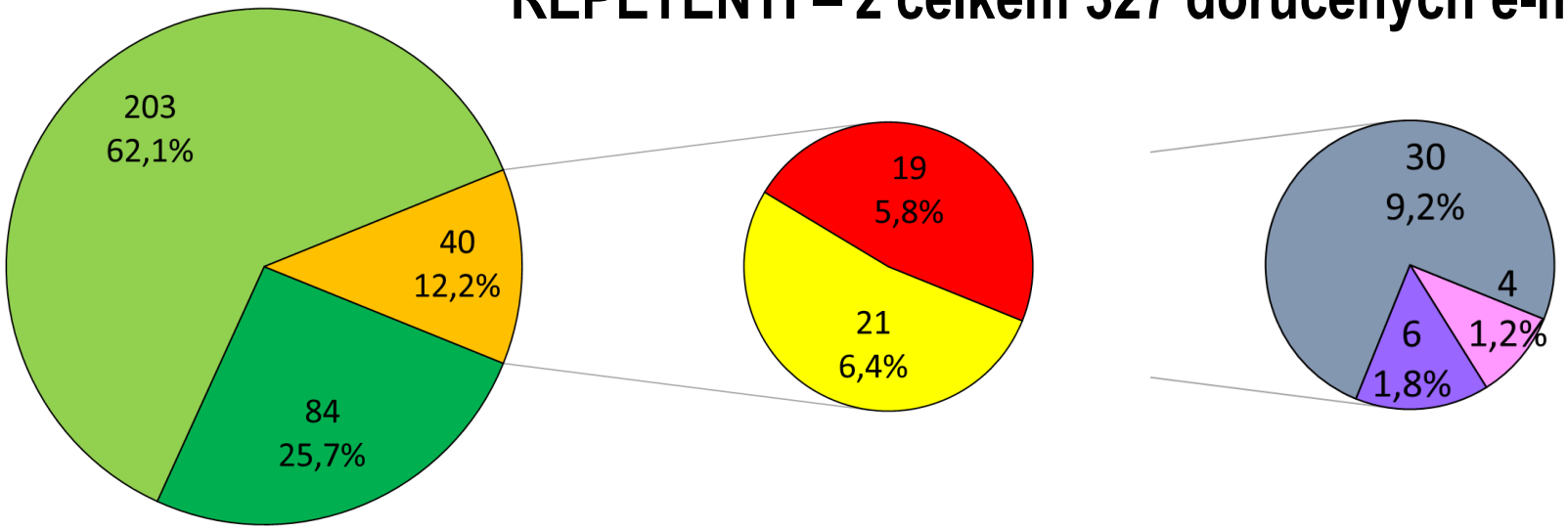


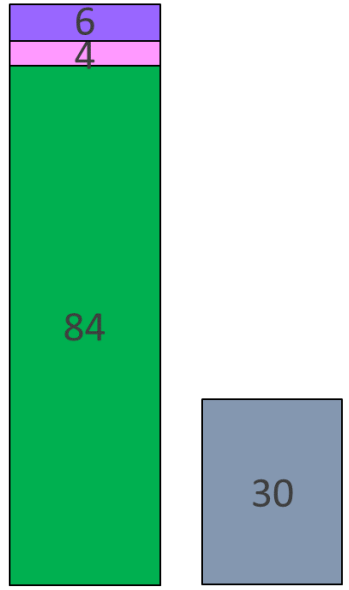


Záznamy v SD

Celkové výsledky phishingových testů 6/2022

REPETENTI – z celkem 327 doručených e-mailů:





NOVÁČCI – z celkem 129 doručených e-mailů: