ATS TELCOM

Riadenie Rizík

v realite prevádzkovateľa základnej služby orgánu verejnej moci z pohľadu manažéra kybernetickej bezpečnosti MKB

ISIT Slovakia s.r.o.
Informačné systémy
Informačné technológie

Verejná správa v SR a kybernetická bezpečnosť

Legislatívne ukotvenie

V existujúcej právnej úprave je orgán verejnej moci (OVM) :
- **prevádzkovateľom základnej služby** podľa zákona č. 69/2018 Z.z. o KB ak prevádzkuje aspoň jednu základnú službu , pričom
- obce a mestá patria do sektoru verejná správa, podsektoru ISVS **ako správcovia alebo prevádzkovatelia ITVS**, , ktorý sa riadi zákonom č. 95/2019 o ITVS.
- pre obce sú definované dopadové kritériá podľa Vyhlášky NBÚ č. 164/2018 Z.z., pričom jedným z určujúcich kritérií je ohrozenie dôvernosti, integrity, dostupnosti a pravosti údajov alebo súvisiacich služieb s dopadom **na viac ako 1000 osôb**

Verejná správa v SR a kybernetická bezpečnosť

Povinnosti , audit a samohodnotenie

Prevádzkovatelia základnej služby **sú povinní** :
- implementovať a dodržiavať bezpečnostné opatrenia rozdelené do 3 kategórií, pričom účelom je zaručiť primeranú mieru odolnosti voči hrozbám a spôsobilosti subjektov

Verejná správa v SR a kybernetická bezpečnosť

Povinnosti , audit a samohodnotenie

Preverenie účinnosti prijatých bezpečnostných opatrení a požiadaviek legislatívy sa vo frekvencii 2 roky vykonáva :

- auditom KB prostredníctvom certifikovaného audítora
- samohodnotením MKB pre I a II. kategóriu podľa postupu NBU , ktoré sa odosiela sa na dozorný orgán – Národný bezpečnostný úrad

Verejná správa v SR a kybernetická bezpečnosť

Možnosti financovania pre orgány verejnej moci

Zistenia z auditov alebo samohodnotení sú podkladom na prijatie účinných opatrení na pokrytie slabých miest a odstránenie nedostatkov.

Spôsob financovania :

1. vlastné zdroje
2. Otvorené 3 výzvy v oblasti KIB v sektore Verejná správa riadiacim orgánom je Ministerstvo investícií, reg. rozvoja a informatizácie SR na regionálnej úrovni v celkovej alokovanej sume **21 mil. eur** (verejná správa, verejné a štátne VŠ, zdravotnícke zariadenia)

Verejná správa v SR a kybernetická bezpečnosť

očakávané zmeny po novele ZoKB (NIS2)

Zmení sa spôsob identifikácie prevádzkovateľov základných služieb (kľúčové a dôležité subjekty) podľa konkrétnych kritérií s rozšírením o nové sektory a regulované služby

Preverenie účinnosti prijatých bezpečnostných opatrení a požiadaviek legislatívy sa vo frekvencii 2 roky zostane zachované (audit a samohodnotenie pre vybrané subjekty) .

Verejná správa v SR a kybernetická bezpečnosť

očakávané zmeny po novele ZoKB

Zruší sa kategorizácia a klasifikácia informácií a informačných systémov.
Nahradí ich ANALÝZA RIZÍK ako univerzálny nástroj pre aplikáciu opatrení
Zefektívni sa hlásenie hrozieb, zraniteľností a Kybernetických bezpečnostných incidentov
Zmení sa sankčný mechanizmus – efektívne vynucovanie pokút ...
Ai ....

Praktický výkon manažéra KB (MKB) súčasný stav

Dôležitosť úkonov MKB

ATS TELCOM

- Identifikačné údaje o organizácii
- Určenie špecifického sektorového a dopadového kritéria
- Presne, detailne odkomunikovaná definícia zadania; musí byť jasne určená
- Identifikácia základných procesov (primárnych aktív),v organizácii slúžiacich pre dosahovanie cieľov alebo splnenie misie organizácie, potrebná spolupráca s DPO (OOÚ)
- Právne predpisy, podľa ktorých sa riadi plnenie misie organizácie
- Údaje o vlastníkovi primárneho / vlastníkoch primárnych aktív
- Identifikácia informačného systému/systémov, od fungovania ktorých priamo závisí základný proces

ISIT Slovakia s.r.o.
Informačné systémy
Informačné technológie

Praktický výkon manažéra KB (MKB) súčasný stav

Dôležitosť úkonov MKB

ATS TELCOM

- Architektúra IS, HLD a LLD design IS (alebo jeho časti) s popisom
- Identifikácia druhov informácií, ktoré sú v IS spracovávané s popisom požiadaviek na ich ochranu (citlivosť informácií), ich dostupnosť a podmienky šírenia
- Informácie o type informačného systému;
- Identifikácia druhov informácií, ktoré sú v IS spracovávané s popisom požiadaviek na ich ochranu (citlivosť informácií), ich dostupnosť a podmienky šírenia
- Voľba bezpečnostného modelu pre informačný systém
- Určenie stupňa bezpečnostných opatrení podľa vybraného bezpečnostného modelu
- Informácie o tretích stranách a ich subdodávateľoch

ISIT Slovakia s.r.o.
Informačné systémy
Informačné technológie

Praktický výkon práce manažéra KB

ATS TELCOM

PROCES SPRACOVANIA A VYHODNOTENIA KOLEKTOVANÝCH INFORMÁCIÍ

Analýza a syntéza

ISIT Slovakia s.r.o.
Informačné systémy
Informačné technológie

Praktický výkon práce manažéra KB

Príklad DÁTOVÝCH TOKOV obce využívajúce cloudové služby DCOM

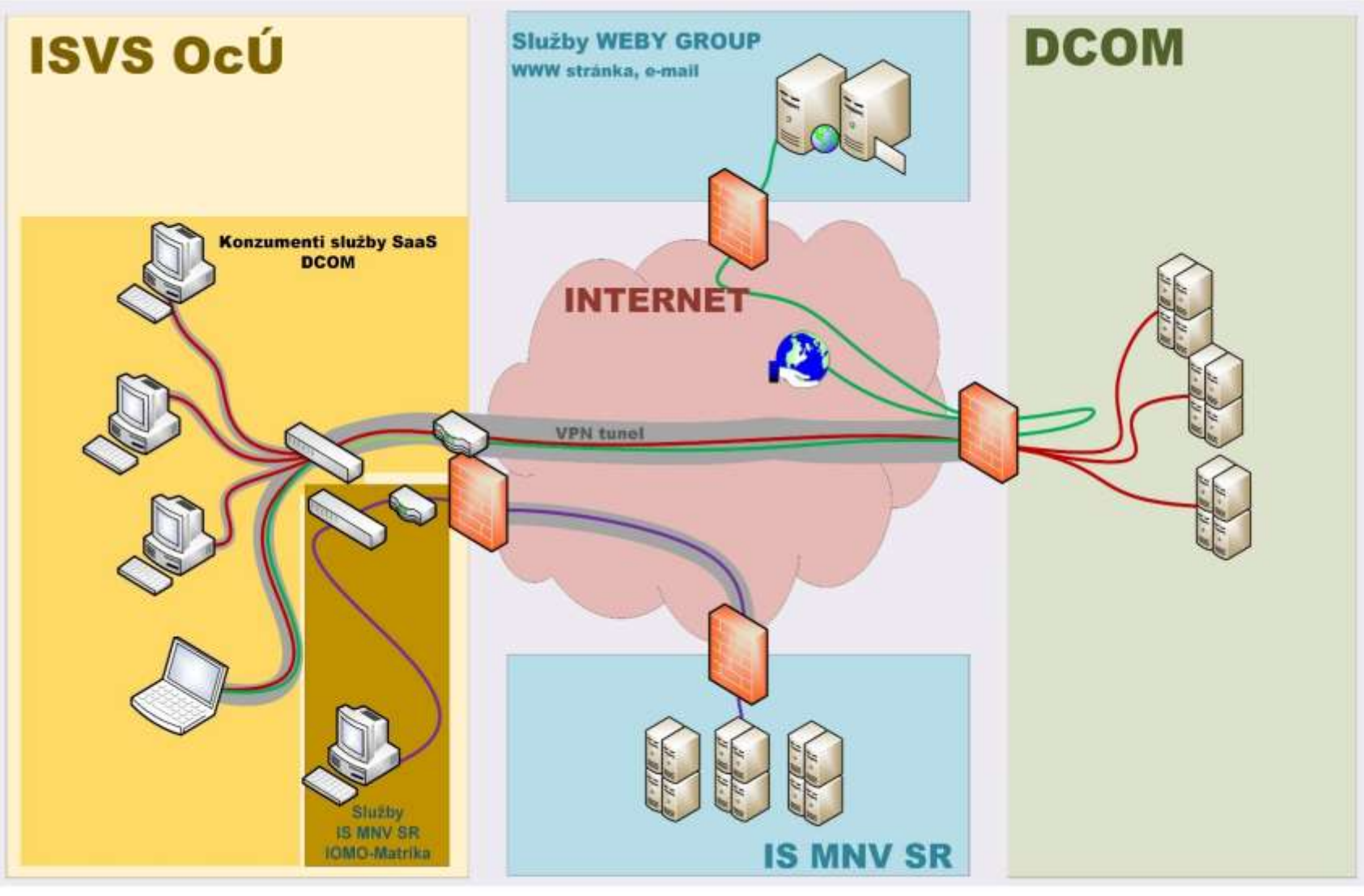
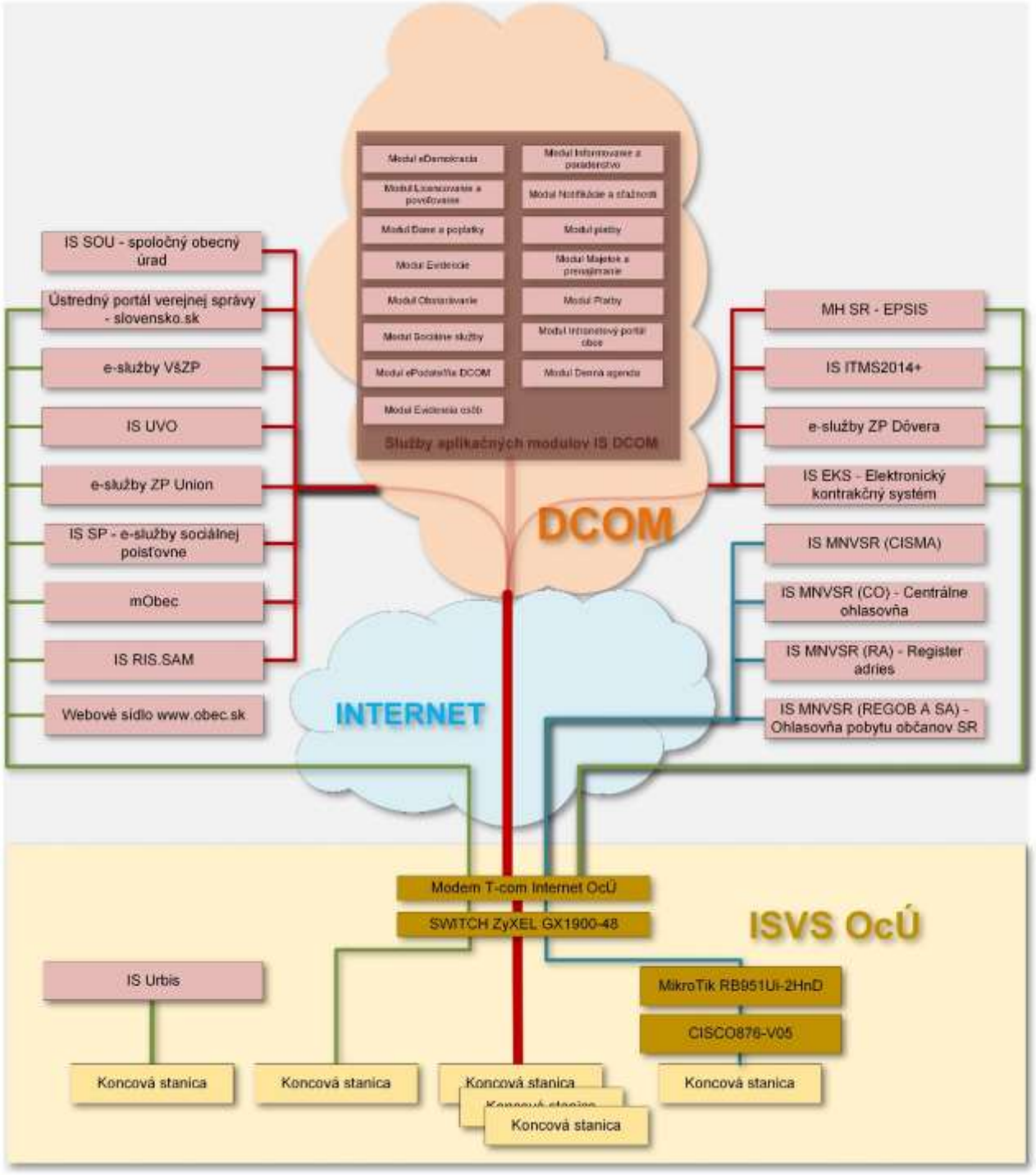


Schéma komunikácie prezentuje oddelenú, chránenú komunikáciu pracovných staníc s konektivitou na cloudovú službu IaaS (IS DCOM).

Z pracovných staníc do prostredia Internetu je umožnený prístup cez chránenú a zabezpečenú infraštruktúru IS DCOM.

Ďalej schéma komunikácie zobrazuje vyčlenenú komunikáciu pracovnej stanice so službami IOMO dostupnými chráneným pripojením na IS MNV SR, pracovná stanica má konektivitu len do prostredia, resp. na služby IOMO IS Min. vnútra SR

Praktický výkon práce manažéra KB
Závislosti primárnych aktív



Aktív = služieb, prostredníctvom ktorých OcÚ zabezpečuje výkon verejnej správy a podporných aktív technickej povahy ISVS OcÚ

Praktický výkon práce manažéra KB

PROCES SPRACOVANIA A VYHODNOTENIA KOLEKTOVANÝCH INFORMÁCIÍ

Ďalší postup

Vstup do procesu analýzy rizík a ich riadenia

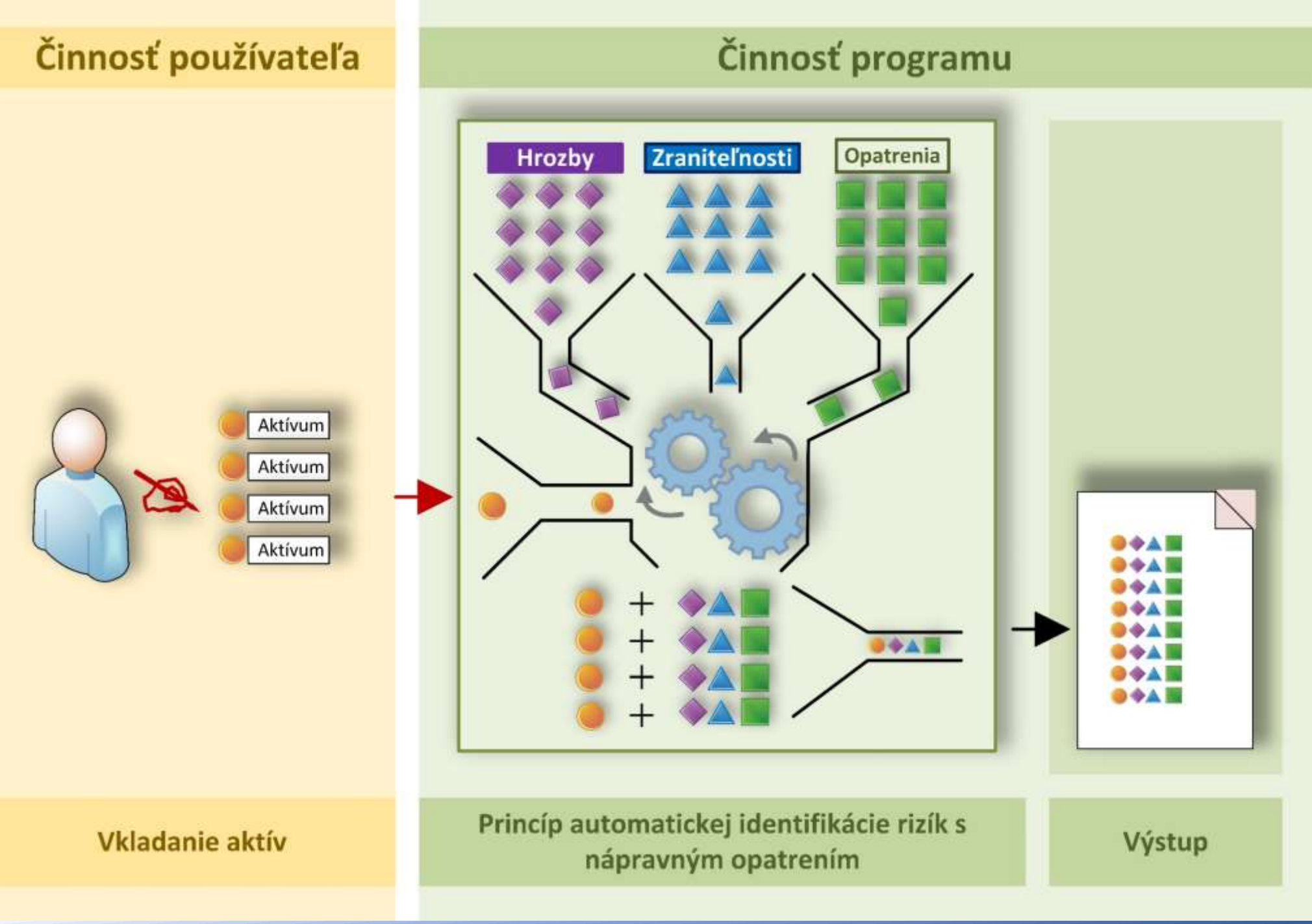
ATS TELCOM

Samotný proces analýzy a riadenia rizík kybernetickej bezpečnosti prevádzkovateľa základnej služby sa riadi právnymi predpismi a metodikami ktoré sú dostatočne detailne spracované a ktoré umožňujú viesť manažéra kybernetickej bezpečnosti celým týmto procesom

ISIT Slovakia s.r.o.
Informačné systémy
Informačné technológie

Praktický výkon práce manažéra KB

Modul KBO automatiz. analýza rizík



Praktický výkon práce manažéra KB

Riadenie aktív a rizík prostredníctvom automatizovaných nástrojov obsahujúcich funkcionalitu :

- Asset management
- **Automatizovaná analýza rizík** s väzbami na ochranné opatrenia
- Dopadová analýza BIA s grafickými výstupmi
- **Konfiguračný manažment CMDB**
- Automatické generovanie záverečnej správy z riadenia rizík, SOA a i.
- Automatizácia bezpečnostných varovaní, management a príjem opatrení z SK-CERT /ENISA
- Komplexný manažment bezpečnostných udalostí / incidentov
- **Riadenie tretích strán** a dodávateľského reťazca
- **Katalóg spracúvaných informácií**

Ďakujem za Vašu pozornosť.

Roman Václav, LL.M, MBA

www.analyza-rizik.eu

Hradec Králové 14. máj 2024