

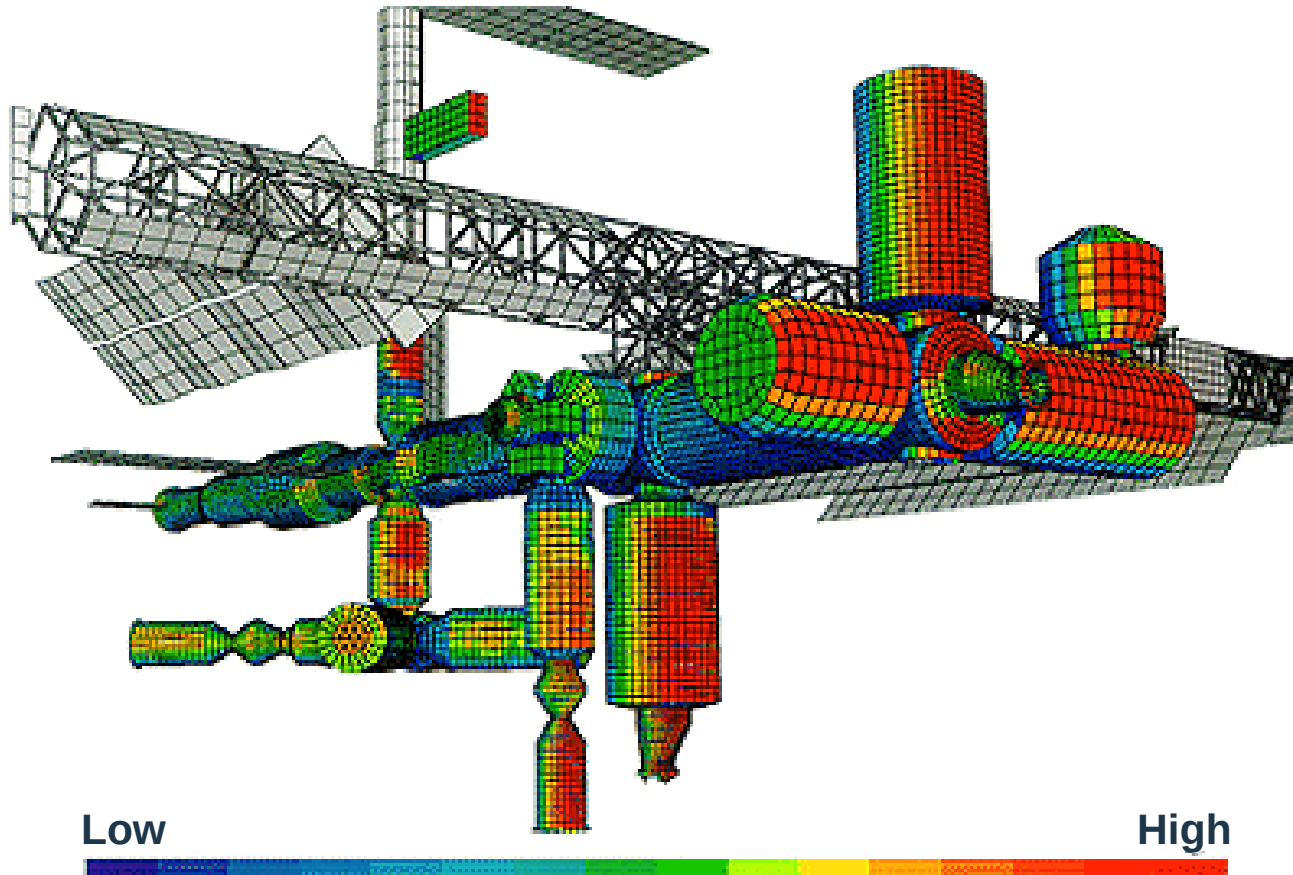
Riadenie bezpečnostných rizík je prevzatie zodpovednosti za realitu

EFOCUS: KRYPTOREALITA A BUDÚCNOSŤ IT BEZPEČNOSTI



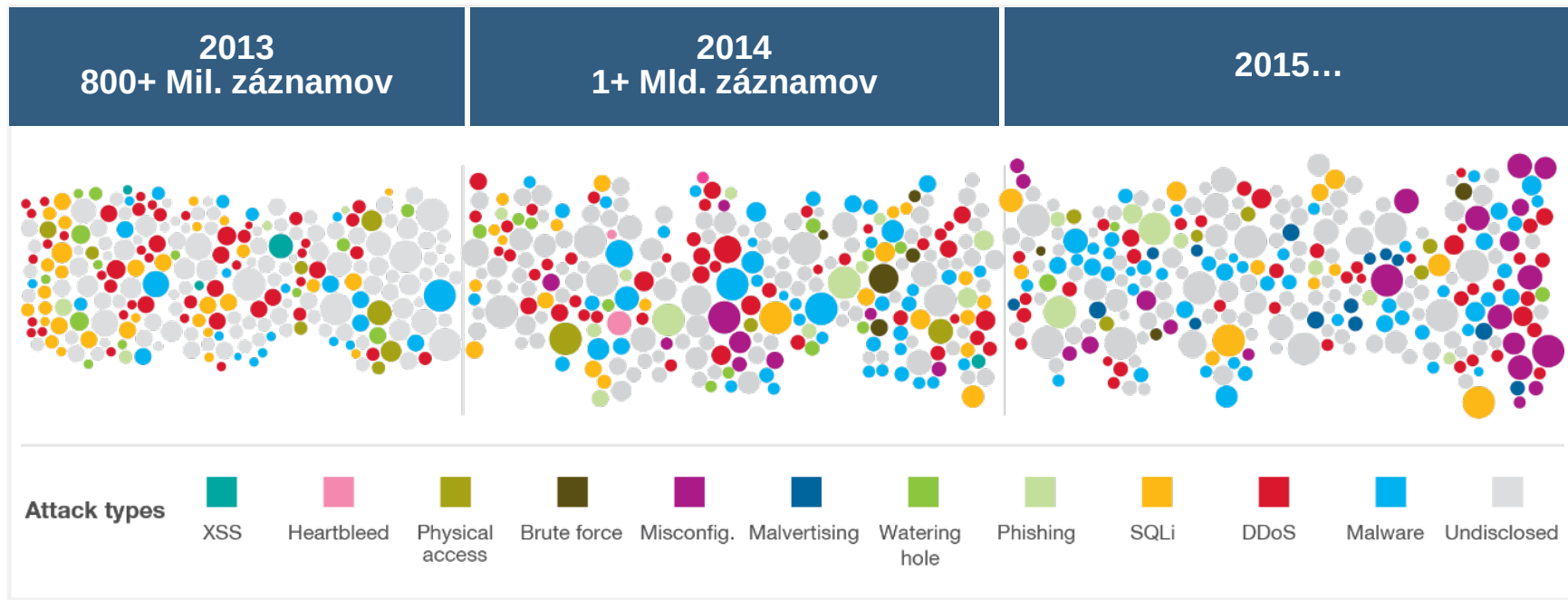
Ivan Makatura
IBM Security Services

NASA model oblastí vysokého rizika na mezinárodní vesmírné stanici ISS



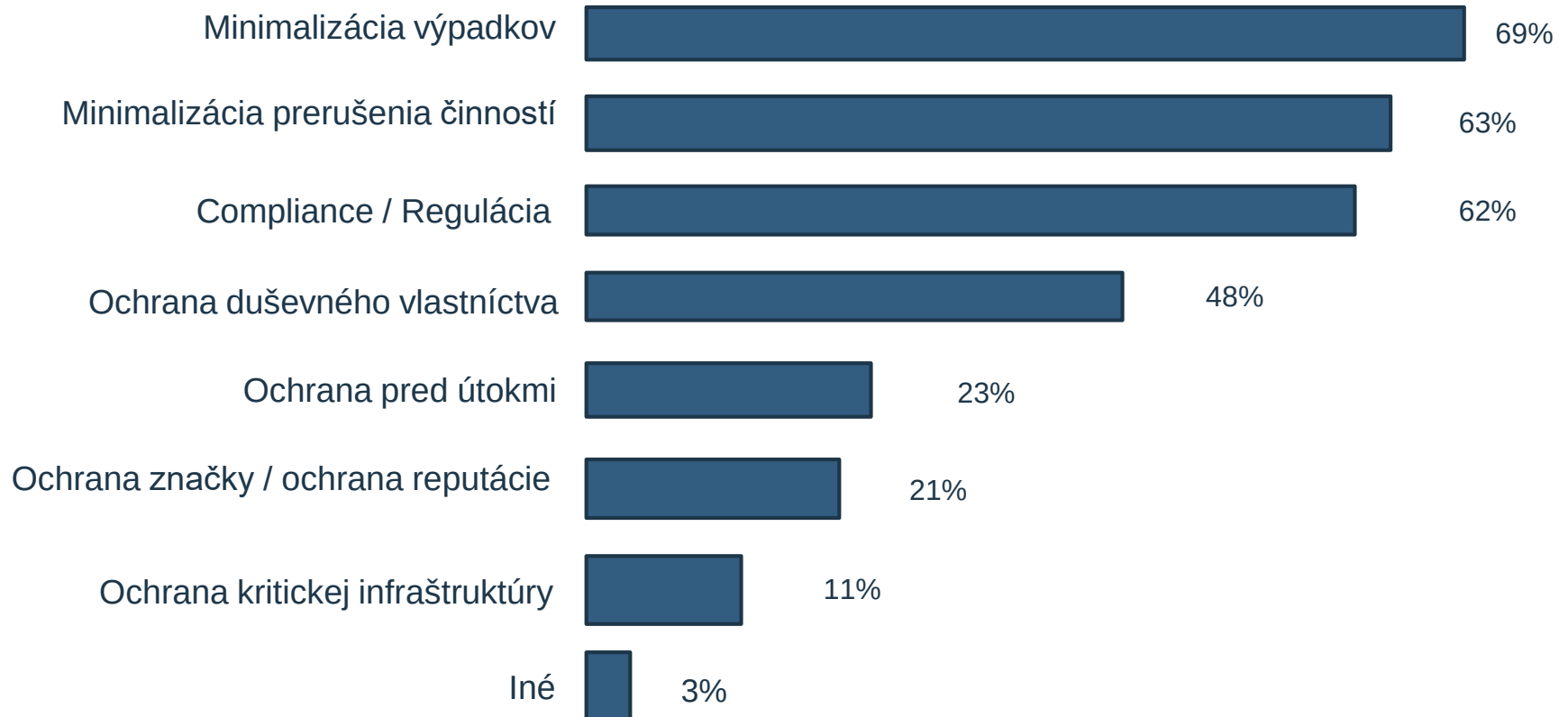
Ak sa rizikom zapodievame v reálnom svete, potom prečo nie aj v tom virtuálnom?

Nárast počtu, objemu a komplexnosti útokov je nespochybniteľný...



Zdroj: IBM X-Force Threat Intelligence Report - 2016

Aké sú typické objektívne dôvody pre riadenie bezpečnostného rizika?



Zdroj: Ponemon's 2016 Application Security Risk Study

Typické motívy zlomyseľného konania

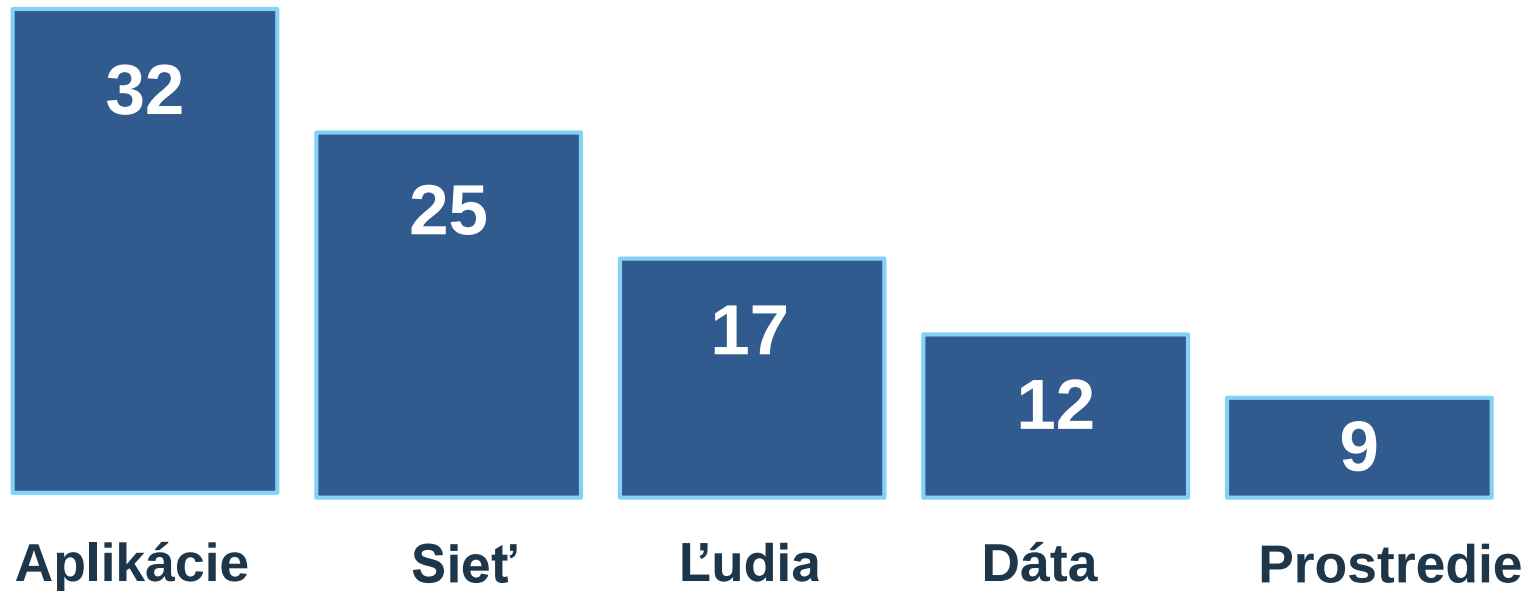
- Zisk
- Vydieranie
- Špionáž
- Sabotáž
- Pomsta



- Politické a sociálne motívy
- Patriotizmus a ideologické motívy
- Ego a samolúbosť
- Trollovia



Aký je najčastejší vektor útokov?



Zdroj: Ponemon's 2016 Application Security Risk Study

Aké sú subjektívne dôvody pre výkon bezpečnostných procesov?

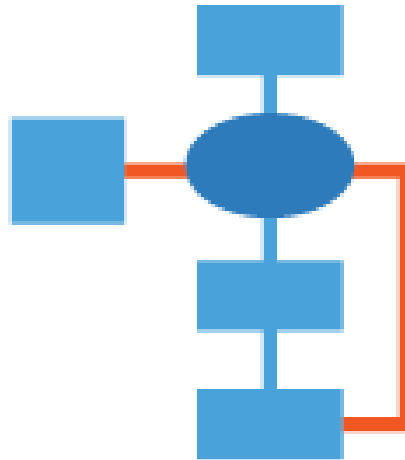


Problémy...

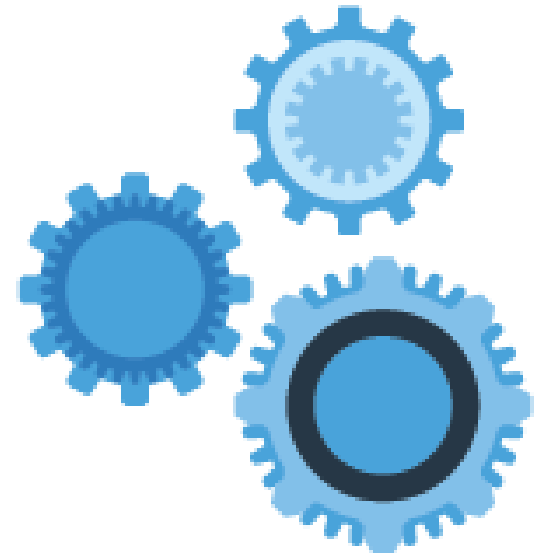
People



Process



Technology



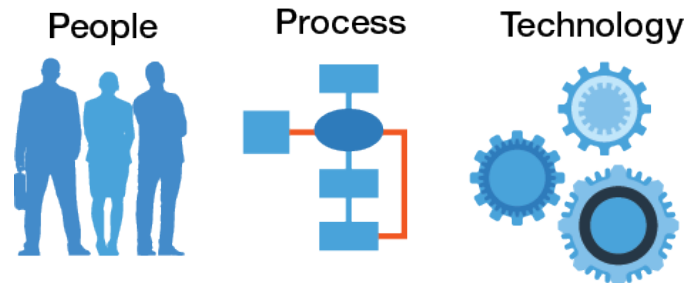
Problém: Ľudia

- **Agresívne prostredie:**

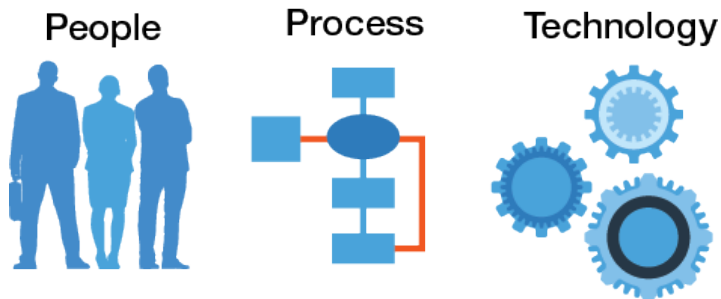
- Stúpajúci počet “hacktivistov”
- Stúpajúca kvalitatívna úroveň kybernetickej kriminality
- Nárast počtu štátmi sponzorovaných profesionálnych hackerov

- **Organizačné dôvody**

- Nie všetci informatici sú zároveň bezpečnostnými špecialistami
- Aj ten najlepšie vyškolený informatik je schopný sa sústrediť len na niekoľko bezpečnostných problémov v tom istom čase
- Systém odmeňovania vo väčšine organizácií je zameraný na výkon, nie na bezpečnosť a opatrné narábanie s rizikami
- Členovia bezpečnostného tímu často pracujú v divíznych „silách“ s malým množstvom efektívnych nástrojov (testovanie zraniteľností, manažment testovania a evidencia rizík)
- Je prirodzenou vlastnosťou človeka podvedomé odmietanie zaoberať sa problémami...



Problém: Proces



- **Biznis:**

- Požiadavky vedenia na zaručenie kontinuity
- Tlak na znižovanie nákladov
- Prednosť má úsilie o tvorbu zisku pred úsilím o ochranu informačných aktív
- Stratu nie je možné exaktne predvídať. Vo chvíli straty si organizácia už len môže priať, aby boli pred udalosťou prezieravo alokované príslušné zdroje

- **IT:**

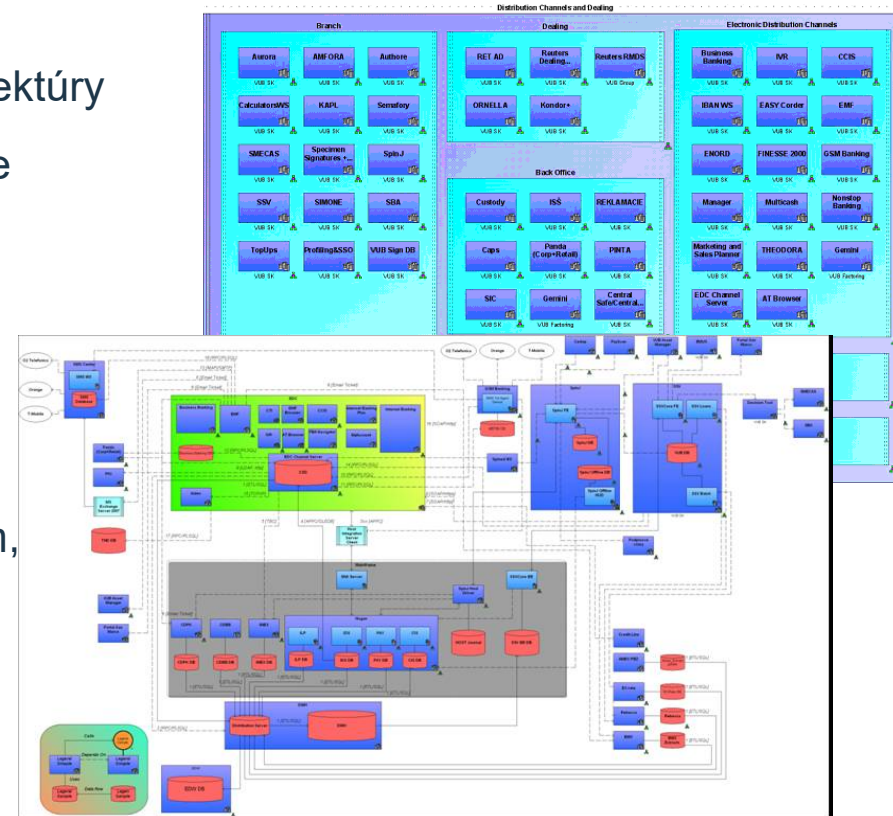
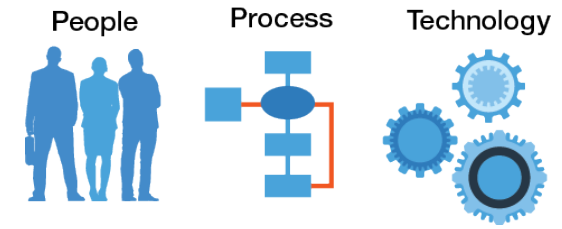
- Pracovná preťaženosť a zahltenie rutinnými činnosťami
- Nedodržiavanie procesu riadenia zmien (výsledok: napr. neexistujúca dokumentácia)
- Obchádzanie politík (napr. chronické nedodržiavanie princípu „Segregation Of Duties“)
- Bezpečnostný incident je neštandardná udalosť, ktorá vyvoláva tendenciu chaotického konania (zvýšené riziko strát)

- **Regulácia:**

- Narastajúca intenzita regulácie (EÚ, SK)
- Odvetvové štandardy

Problém: Technológia

- Nové produkty generujú nové požiadavky na ich podporu zo strany IT prostriedkov
- Tlak biznisu na nové funkcionality znamená mnohokrát chaotické zmeny aplikačnej architektúry
- Zvyšujú sa nároky na prepojitelnosť, zdieľanie zdrojov a mobilitu
- Rastúce možnosti prepájania významným spôsobom zvyšujú komplexitu IT riešení
- Aj jediná chyba môže viesť kritickej zraniteľnosti
- Technológie sú využívané aj takým spôsobom, ktorý ich tvorcovia pôvodne nepredpokladali (napr. Bluetooth, GSM SMS, univerzálne využitie IP protokolu atď.)



Výsledok tohto prístupu ku riadeniu bezpečnosti...

- Máloktorý podnik má úplný prehľad o stave a vývoji bezpečnosti naprieč všetkými procesmi
- Nie je k dispozícii žiaden formálny mechanizmus rozhodovania o bezpečnostných prioritách v podniku
- Nejestvuje konsolidovaná metrika pre bezpečnosť
- Iba v máloktorom odvetví jestvujú formálne postupy pre zladenie bezpečnostných aktivít s obchodnou stratégiou
- Zdroje sú zmrazené v „silách“ a väčšinou zložité ich realokovať podľa potrieb

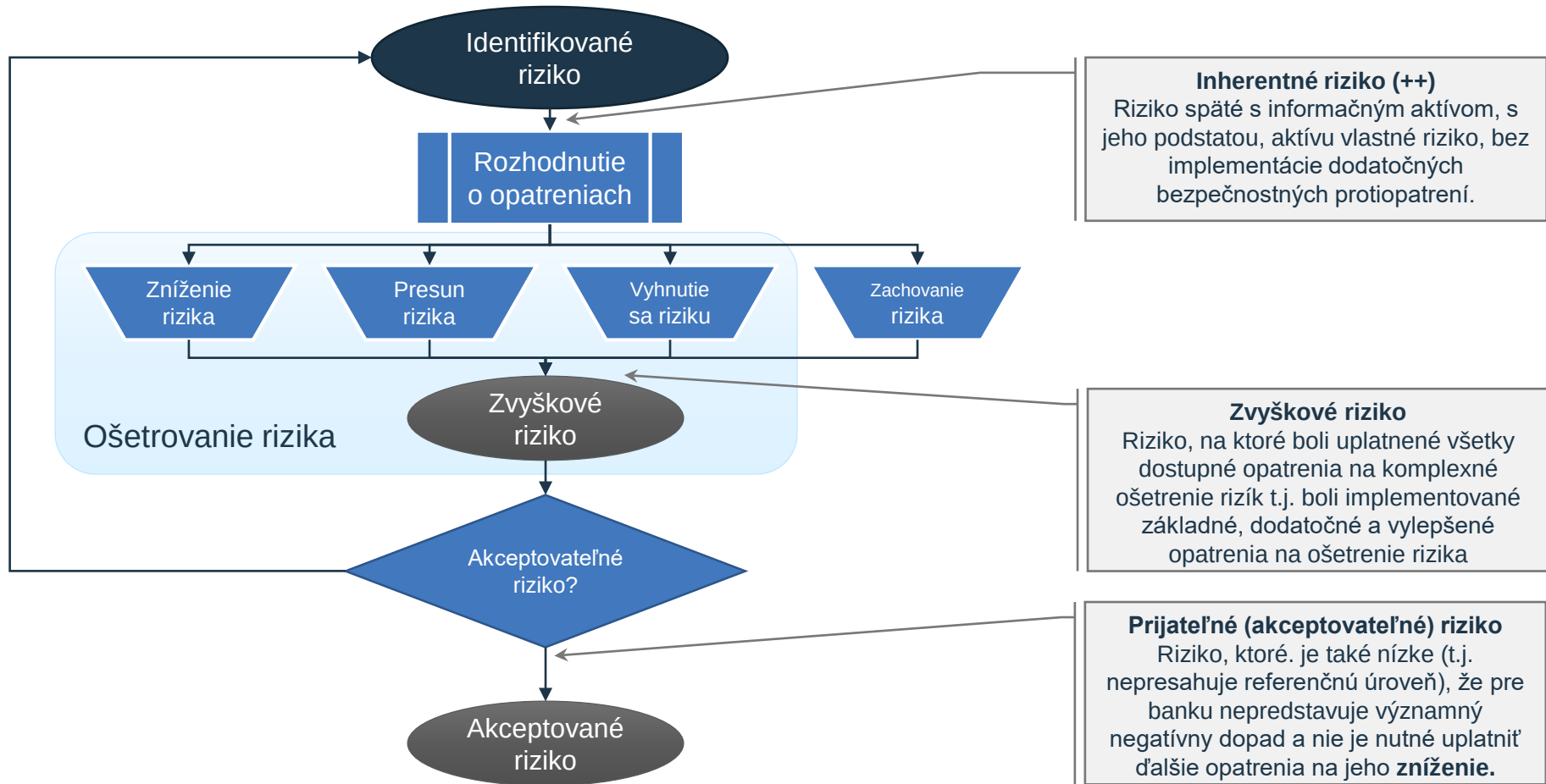




Poznáme výsledok, i dôvody...
Čo s tým urobiť?

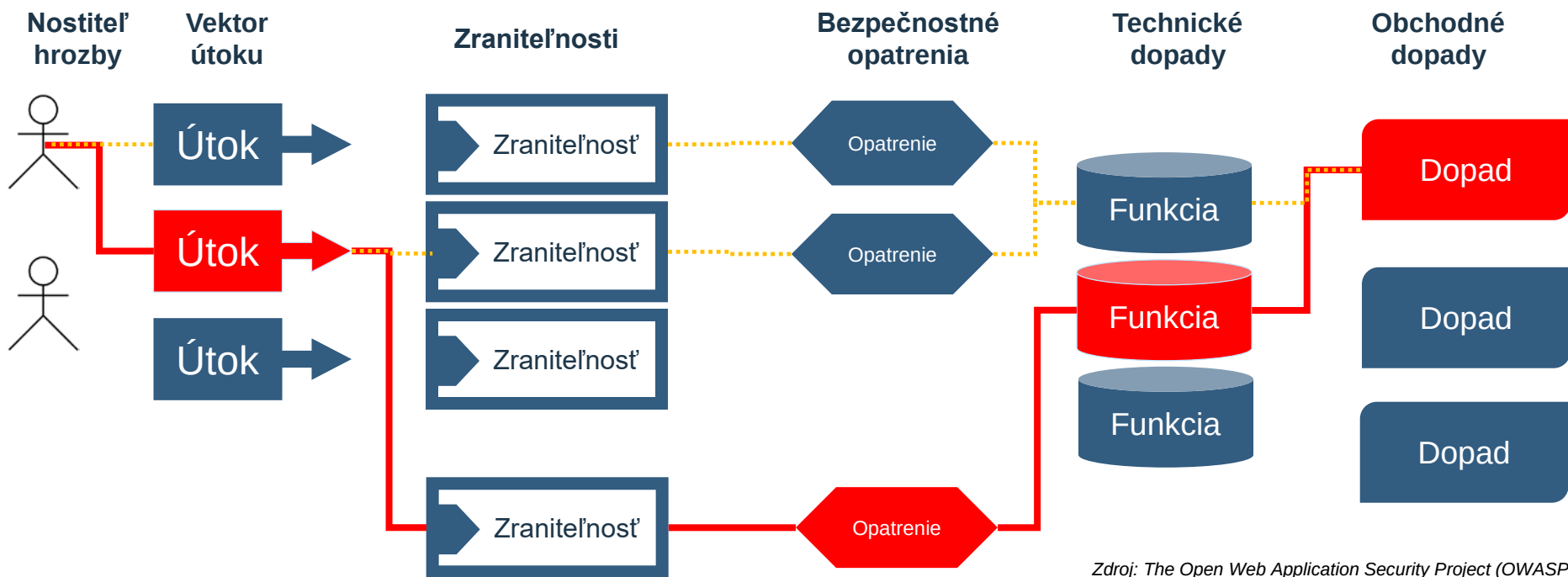


Proces ošetrovania rizika



Čo je to bezpečnostné riziko aplikácie?

- **Vektor útoku** - smer interakcie, súhrn všetkých vstupno-výstupných bodov prostredia, prostredníctvom ktorých sa neoprávnený užívateľ môže pokúsiť zadať alebo extrahovať dáta (v prenesenom zmysle každá cesta, spôsob, mechanizmus, ktorý útočník môže zneužiť na neoprávnený prístup k informačným aktívam)
- **Zraniteľnosť** - slabé miesto informačného aktíva, slabina v informačnom systéme, v bezpečnostných procedúrach systému, opatreniach alebo implementácii, ktoré môže aktivovať alebo využiť nositeľ hrozieb



Zdroj: The Open Web Application Security Project (OWASP)



Päť krokov k riadeniu bezpečnosti založenom na riadení rizika



Krok1: Vytvorte aplikačné profily



- **Šablóna profilu aplikácie/systému:**
 - **Základná identifikácia:**
 - názov aplikácie
 - vývojársky tím
 - zodpovedný biznis útvar
 - meno vlastníka procesu (“business owner”)
 - **Atribúty inherentného rizika:**
 - Jedná sa o klientskú aplikáciu? Internú podpornú aplikáciu atď.
 - Technická špecifikácia, miera funkčnej zložitosti aplikácie
 - Miera infraštruktúrnej zložitosti
 - Vypelosť aplikácie (ako dlho je aplikácia v živej produkcii?)
 - Platforma (web/klient-server/desktop/mobilná)

Krok1: (Aplikačné profily) Posúďte možné dopady rizík na biznis



- **BIA = Business Impact Analysis**
- Pri posudzovaní kritičnosti biznis aplikácií je potrebné vziať do úvahy potenciálny dopad na prerušenie prevádzky:
 - pravdepodobnosť rizík, vrátane reputačného rizika
 - odhad potenciálu prerušenia prevádzky:
 - požiadavky na dostupnosť
 - Hodnoty RTO a RPO
 - odhadované náklady na prípadné pokrytie strát vzniknutých z prerušenia prevádzky
 - Môže prípadný incident spôsobiť porušenie zmluvných záväzkov?
 - Môže prerušenie spôsobiť právnu zodpovednosť voči zákazníkom a obchodným partnerom?
 - požiadavky na súlad
 - popis kategórií citlivých údajov
 - právne a zmluvné povinnosti

Krok2: Testovanie zraniteľností



- **Statická analýza**

- (niekedy nazývaná aj “white-box analýza”) preskúmava zdrojový kód aplikácií na potenciálne zraniteľnosti
- uľahčuje detekciu bezpečnostných zraniteľností v ranej fáze vývojového cyklu

- **Dynamická analýza**

- (tiež “black-box”), analýza testuje spustené aplikácie “zvonku”
- simuluje mnohé z techník ktoré používajú útočníci

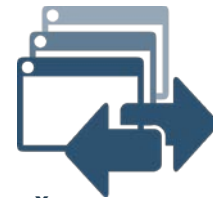
- **Interaktívna analýza**

- (tiež „grey-box“, alebo “glass-box”) analýza testuje aplikácie umiestnením runtime agentov na serveroch, kde sú aplikácie spustené
- preskúmava aplikácie v rámci vlastného aplikačného prostredia a jeho najbližšieho okolia
- Spája v sebe aspekty statickej a dynamickej analýzy umožňujúc detekciu väčšieho množstva bezpečnostných zraniteľností

- **Analýza mobilných aplikácií**

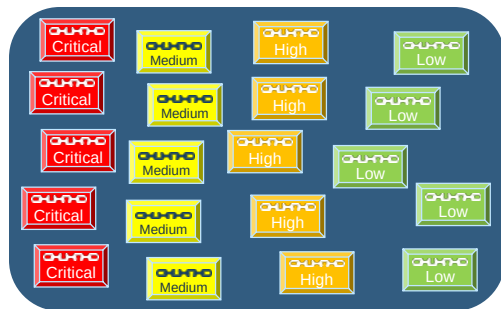
- preskúmava kód, ktorý je sťahovaný na klienta použitím mobilných a koncových systémov

Krok3: Prioritizácia zraniteľností



Obchodné dopady

Súlad
Reputácia
Citlivé údaje
Vplyv na zákazníka
Interný vplyv
Platforma
Zložitosť



- Dobrou praxou v tomto procese je vypočítať celkovú úroveň zraniteľnosti pre každú aplikáciu / systém zvlášť
- Úroveň rizika je potom založené na vzorci:

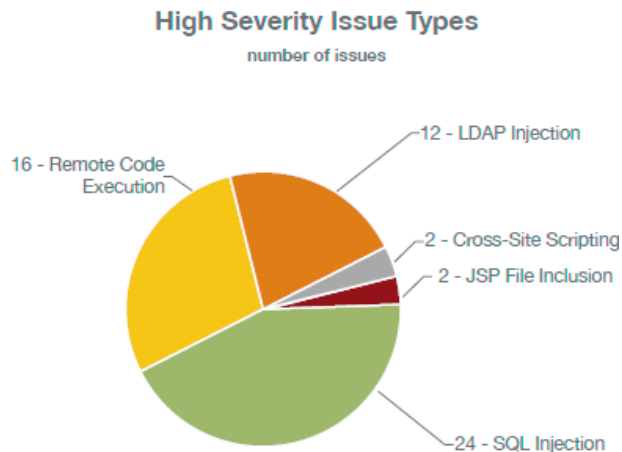
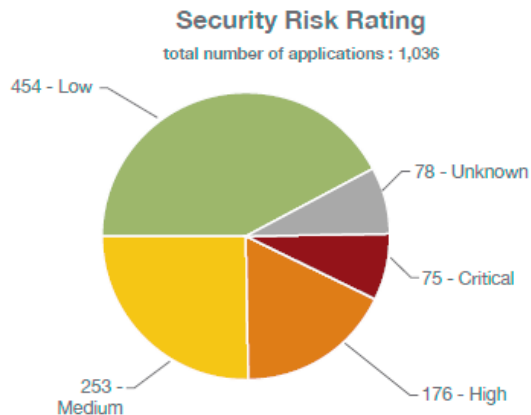
Security risk rating =

Business Impact x

Maximum Vulnerability Severity

- Kde
 - „**Business Impact**“ (dopad) je kalkulovalý na základe hodnotenia rizika a BIA
 - **Maximum Vulnerability Severity (Maximálna kritičnosť zraniteľnosti)** je úroveň najvyššej vyhodnotenej zraniteľnosti nájdennej v rámci aplikácií (Critical/High/Medium/Low/None)

Krok 3: Prioritizácia zraniteľností

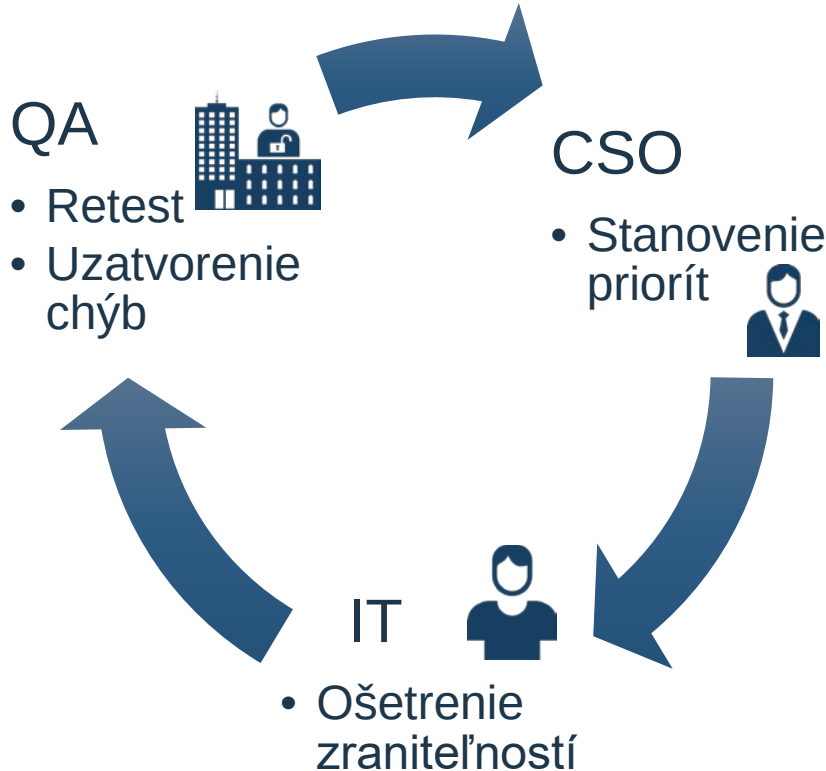
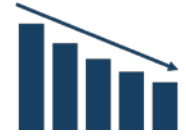


Applications

Total Applications **13**

Summary					
Add Filter...					
Name	Type	Business Impact	Tested	Business Unit	Business Owner
AuthenticationMaster SSO 1.05	Web	Critical	No	Commercial Transportation	Elias Kyger
ghost	Web	Critical	Yes	Commercial Transportation	Elias Kyger
JavaBB	Web	Critical	No	Commercial Transportation	Elias Kyger
joomla	Mobile	Critical	Yes	Commercial Transportation	Elias Kyger

Krok 4: Ošetrovanie zraniteľností

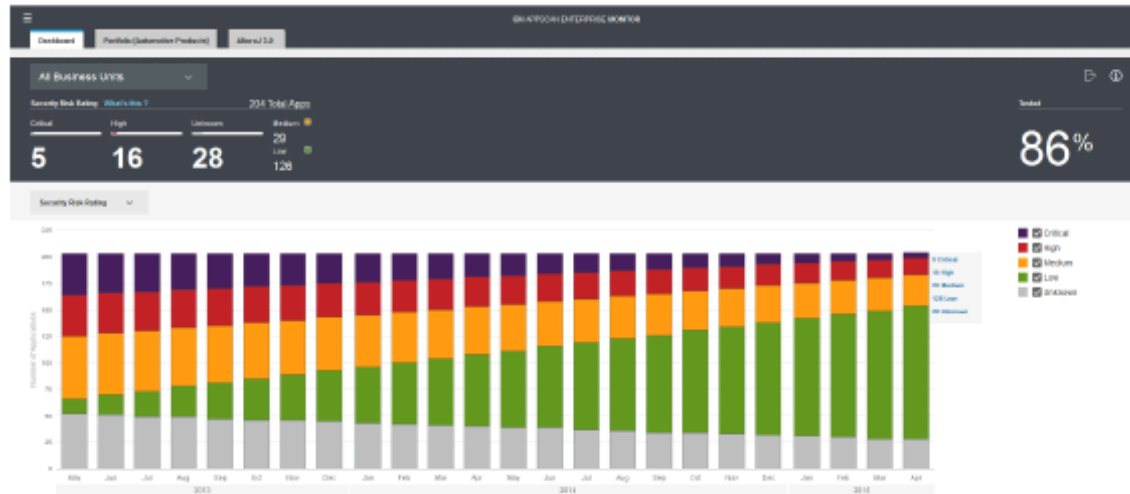


- Manažér bezpečnosti stanovuje priority pre ošetrovanie zraniteľností
- IT manažéri riadia vlastníctvo úloh
- IT (vývoj, prevádzka) sa sústreďujú na nápravu zraniteľností z najvyššou prioritou
- Manažér testovania riadi príslušné testovacie procedúry pre každú novú verziu systému
- Potvrdzuje, že opatrenia sú účinné a odovzdáva výsledky testovania bezpečnostnému manažérovi

Krok 5: Sledujte progres a demonštrujte súlad



- Ak má bezpečnostný manažér k dispozícii kvalitné výstupy aplikačného testovania, je možné zodpovedať na otázky:
 - Zlepšuje sa celková riziková expozícia podniku?
 - Priradujeme zdroje tam, kde majú najväčší vplyv na zníženie rizika?
 - Dokážeme predstavenstvu deklarovat' pozitívne výsledky?
 - Dokážeme od predstavenstva získať zdroje na ďalšie ošetrovanie rizika tam kde je to potrebné?

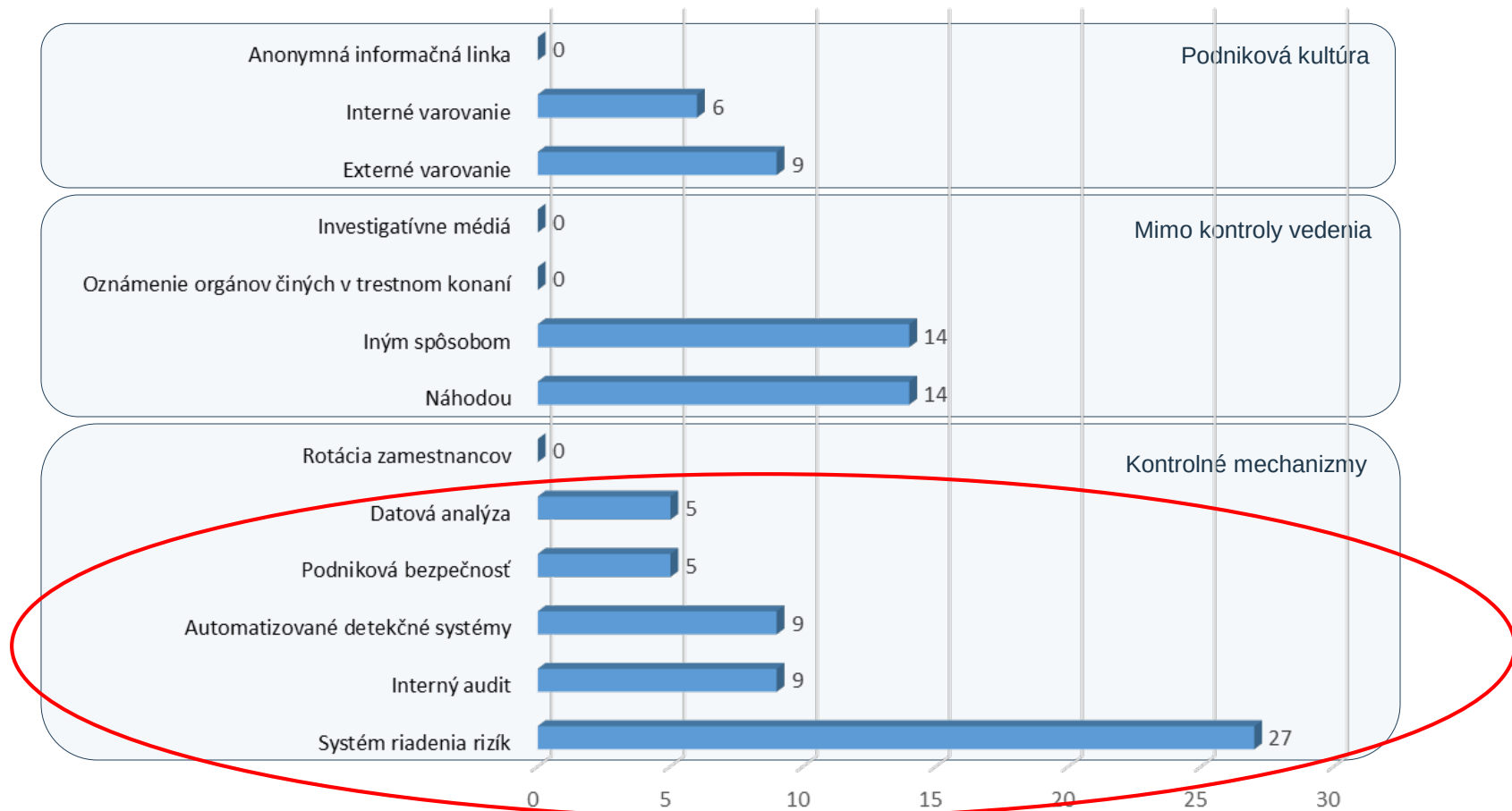




Záver



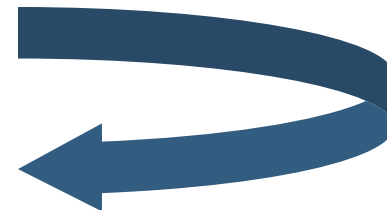
Spôsoby odhaľovania incidentov



Zdroj: „Globálny prieskum hospodárskej kriminality“ © PwC 2014



- Bezpečnosť založená na riadení rizika môže organizáciám napomôcť:
 - získať prehľad o stave zabezpečenia aplikácií v rámci celého podniku
 - stanovovať priority pre testovanie a ošetrovanie zraniteľností, ktoré budú v súlade s obchodnou stratégiou podniku a rizikovým apetítom
 - pridelovať zdroje čo najefektívnejšie, s cieľom zabrániť narušeniam z najvyššou pravdepodobnosťou a najväčším dopadom
 - hodnotiť progres ošetrovania zraniteľností v kontexte bezpečnostných cieľov
 - posilniť spoluprácu medzi bezpečnosťou a IT
 - zlepšiť monitorovanie prevádzky produkčných systémov
 - priebežne sledovať celkovú rizikovú expozíciu podniku



Riadenie bezpečnostných rizík je prevzatie zodpovednosti za realitu

ĎAKUJEM ZA POZORNOST

 ibm.com/security
 securityintelligence.com
 xforce.ibmcloud.com
 [@ibmsecurity](https://twitter.com/ibmsecurity)
 ivan.makatura@sk.ibm.com

© Copyright IBM Corporation 2016. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. Any statement of direction represents IBM's current intent, is subject to change or withdrawal, and represent only goals and objectives. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.