Security Expert Center (SEC)

Jiná dimenze v IT bezpečnosti

Jiří Sedlák

Ředitel, Security Expert Center

11.5.2016

O2 IT Services

Kybernetické útoky všude kolem nás

Kybernetické útoky způsobily v posledních 12 měsících evropským firmám ztráty ve výši **62 miliard dolarů**

Průměrný kybernetický útok stojí podnik **1,2 procenta příjmů**

Napadena může být **každá šestá firma nebo organizace**

Nejedná se jen o náklady finanční, ale také o **vážné poškození pověsti nebo zcizení osobních dat**

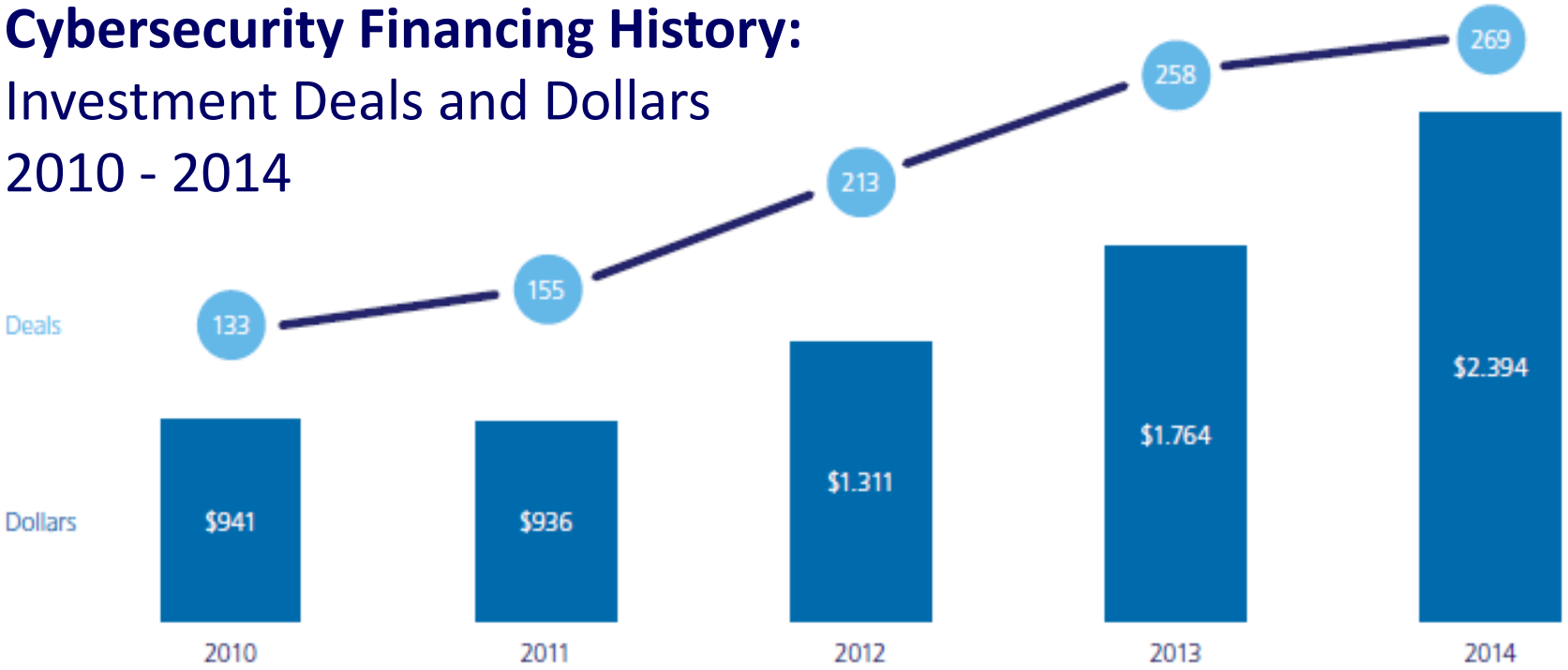
Téměř polovina organizací se však nadále vystavuje riziku tím, že nemají **žádnou komplexní strategii** pro prevenci kybernetické kriminality

Zdroj: Grant Thornton (2015)

O2 IT Services

Vývoj investic v oblasti bezpečnosti IT

Cybersecurity Financing History:
Investment Deals and Dollars
2010 - 2014



Zdroj: cbsinsights.com

O2 IT Services

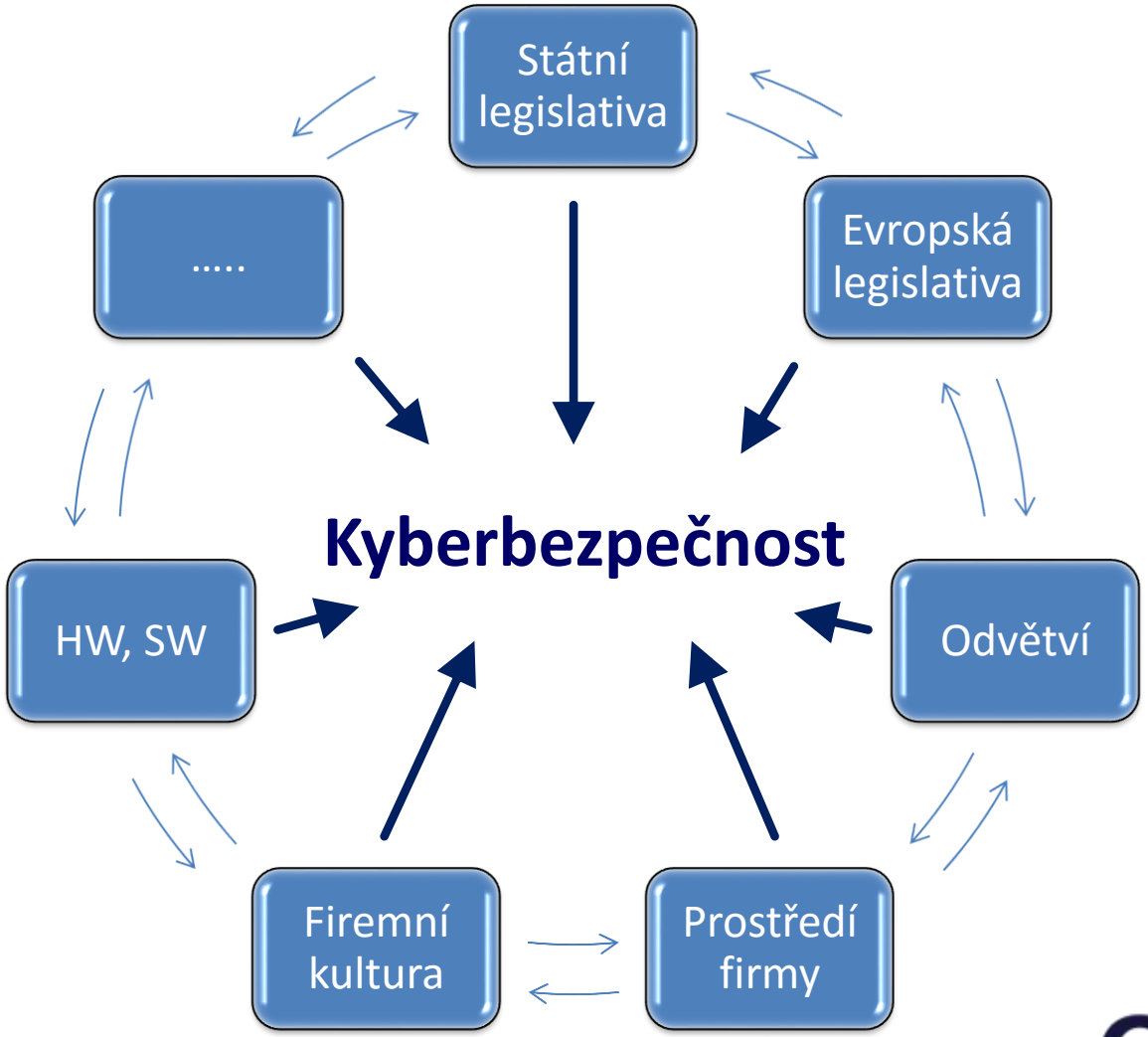
„CIA“ triáda

Informační bezpečnost, jak vyplývá ze standardu **ISO IEC 27000**, znamená zajištění ochrany informací z hlediska jejich:

- ✓ **důvěrnosti**
  (informace pouze pro autorizovaného uživatele)
- ✓ **integrity**
  (přesnost a úplnost informace a metod jejího zpracování)
- ✓ **dostupnosti**
  (dostupnost informace pro oprávněné uživatele, když je potřebují)

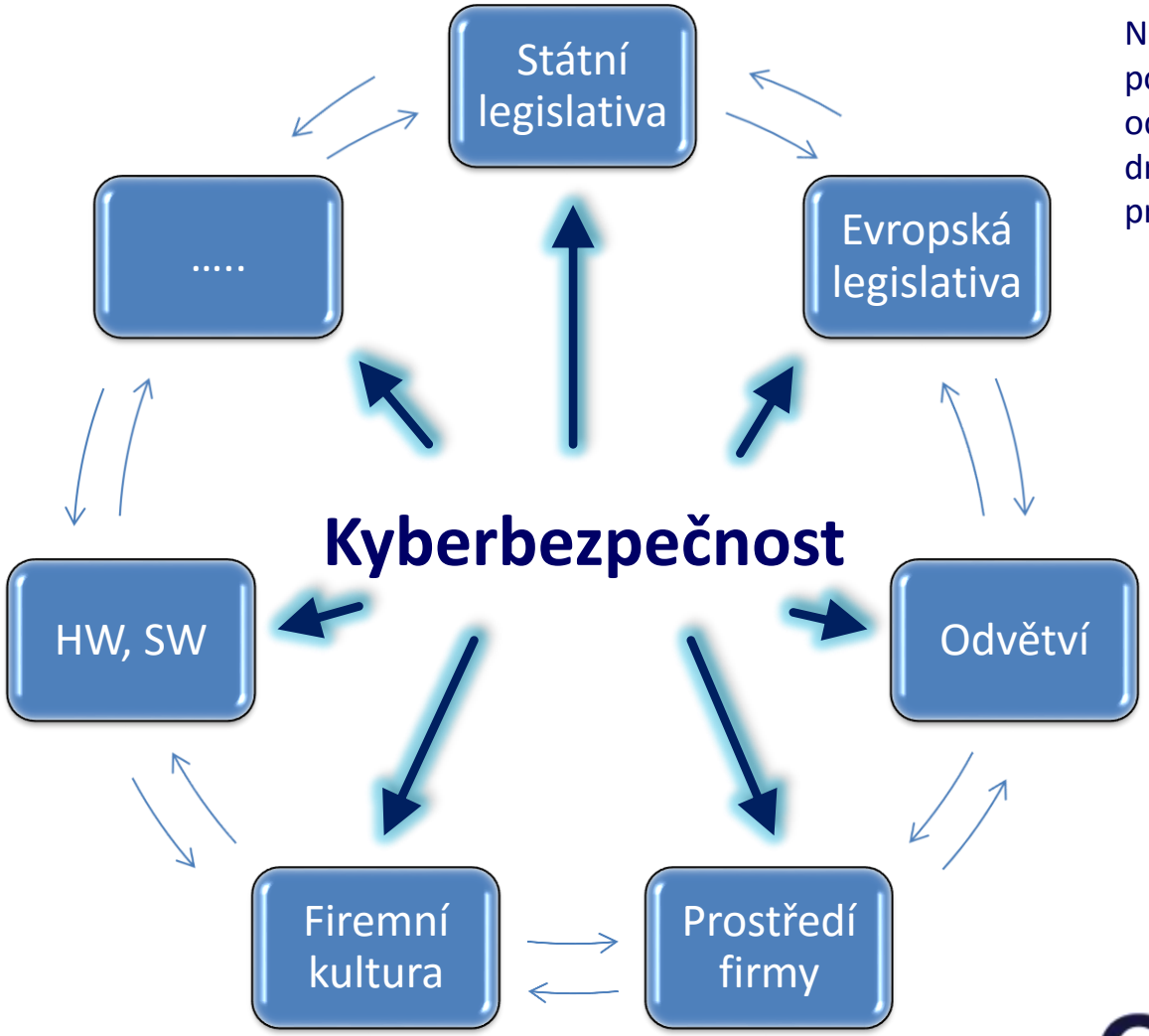
O2 IT Services

Kybernetická bezpečnost = multidisciplinární obor



O2 IT Services

Kybernetická bezpečnost není jen o IT !!!



Nové legislativní požadavky – právní odpovědnost za nehody, drony, řízení leteckého provozu, ...

Zdravotnictví, doprava, automotive – next generation cars, Smart City, ...

O2 IT Services

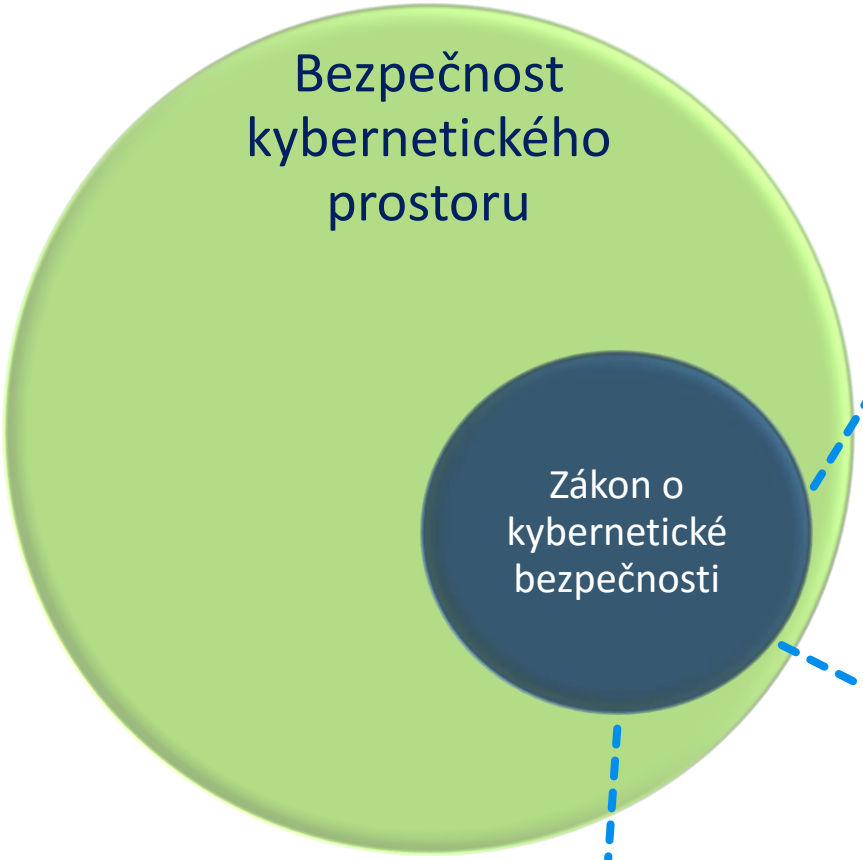
Jak můžeme zajistit informační bezpečnost?

- Integrací architektury, ve které kombinace aplikací, systémů, řešení, softwarů, reportů, alertů a zranitelností pracují společně
- Zajištěním monitoringu v režimu 24x7
- Zajištěním expertních zdrojů, procesů, technologií, politik, prostředků, postupů a dokumentace

Bezpečnost řešení tedy není jen bezpečnost systému a zařízení!

O2 IT Services

Kyberzákon vs. kyberbezpečnost



Subjekty
- Státní orgány
- Vlastníci kritické a významné infrastruktury
- Orgány státní moci
- Komerční subjekty

!!! SPOLUPRÁCE A SDÍLENÍ INFORMACÍ !!!

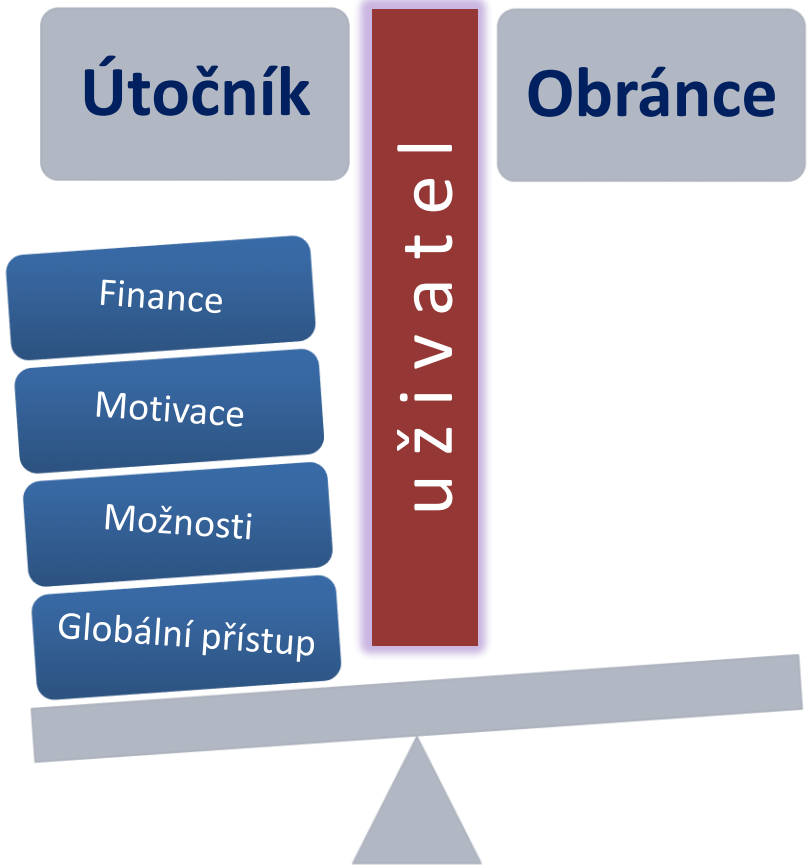
Vazba – ostatní legislativa a EU legislativa (nové normy NIS, GRDC a jejich dopady)

Rozsah – nástroj pro uplatnění a vymáhání kybernetické bezpečnosti v určitých oblastech

O2 IT Services

Puzzle kybernetické bezpečnosti v ČR

Kdo má navrch?



O_2 IT Services

Schizofrenie bezpečnostního ředitele

Pár faktů .....

- Informační bezpečnost je ORGANIZAČNÍ PROBLÉM, nikoliv IT PROBLÉM
- Více než 70% hrozeb jsou INTERNÍ
- Více než 60% viníků jsou kriminální „panici“
- Největší riziko: LIDÉ
- Největší hodnota: LIDÉ
- Sociální engineering je vážná hrozba
- Více než 2/3 dotazovaných společností není schopno rozpoznat „zda jsou jejich systémy kompromitovány”

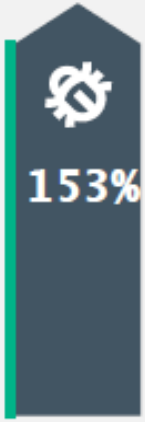
O2 IT Services

HPE Cyber Risk Report 2016

Over one-third of the applications scanned – 35 percent – exhibited at least one critical- or high-severity vulnerability.

Nearly **86%** of enterprises surveyed state they are using IDS.

The use of open source components in applications has increased. **14%**



Over 10,000 new threats were discovered daily on the Android platform, reaching a total year-over-year increase of 153%.

80%

Over 80% of open source and commercial applications suffer security feature vulnerabilities, with serious implications for management of private data.

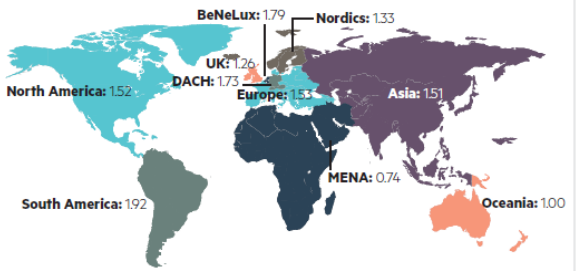
With 95% of newly discovered malware samples and 42% of exploits targeting Windows, that OS remains the dominant platform for attack.

Mobile applications that suffer from internal system information leaks highlight the concern for storing business critical data on easily lost devices.

29% of all exploit samples discovered in 2015 continued to use a 2010 Stuxnet infection vector that has been patched twice.

2016 State of Security Operations

154 assessments in 26 countries



Major findings

The **#1 concern** is access to **skilled resources**

24% not providing minimum security monitoring capabilities

85% not achieving recommended maturity levels

Trends

- Hunt teams and analytics
- Security orchestration and automation
- Hybrid staffing and infrastructure models
- Intelligence sharing

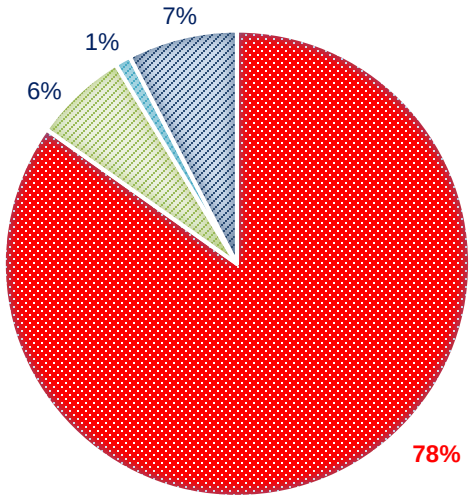
2015 SOMM Trend

Overall ↓	Energy ↓	Financial ↓	Government ↓	Healthcare ↓
Retail ↓	Services ↑	Telecom ↓	Technology ↓	Manufacturing —

O2 IT Services

Kdo zodpovídá za informační bezpečnost?

Útvar IS/IT	78%
Útvar bezpečnosti	6%
Útvar auditu	1%
Žádný útvar	7%



… Je to správný model?

O2 IT Services

Think about the box

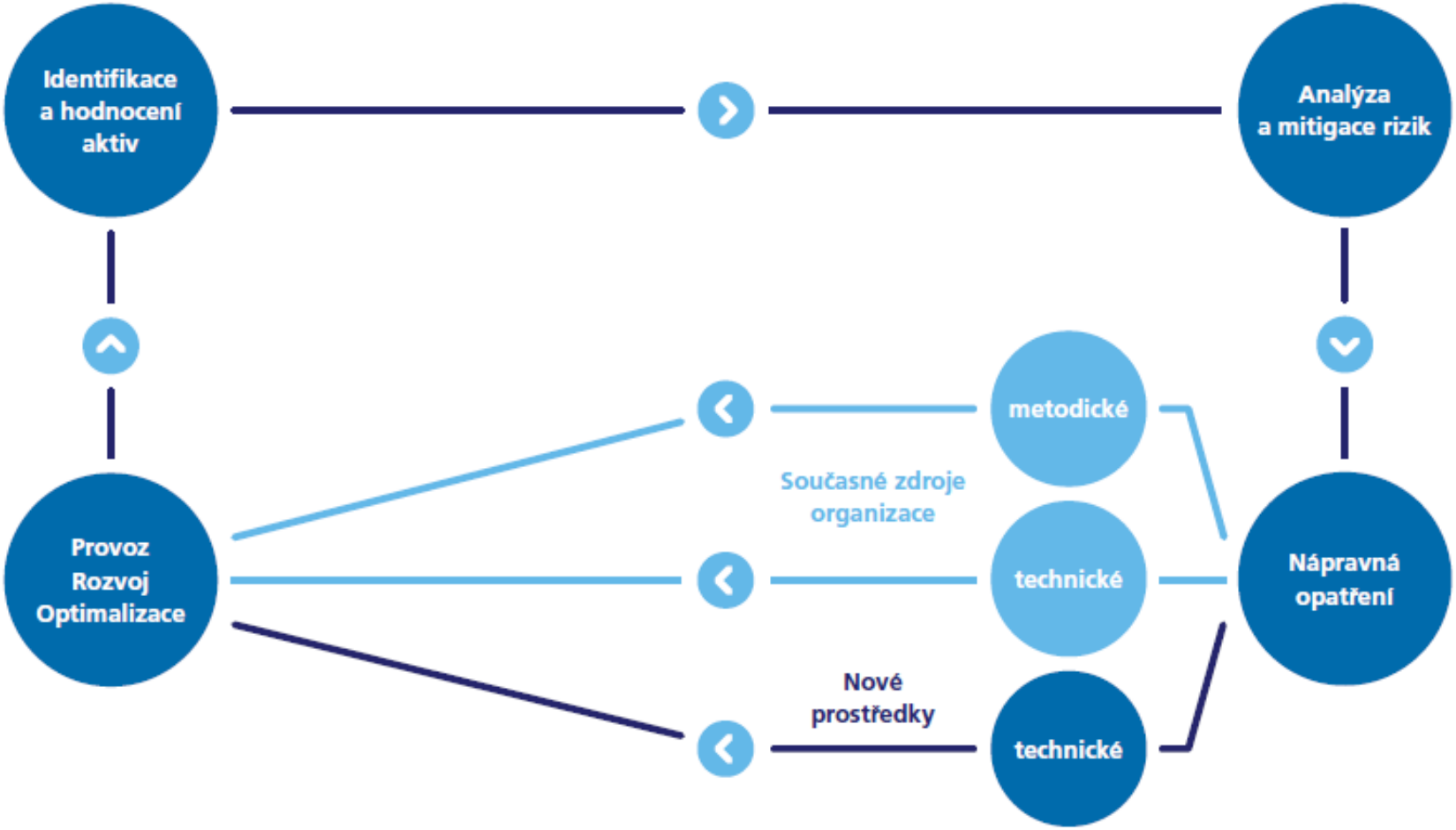
Aktiva společnosti:
Znáte je? Chráníte je? Máte je zhodnocená?

- Máte na to **lidi** … Kolik?
- Máte zajištěné jejich **vzdělávání** … Jak?
- Máte na to **techniku** … Jakou?
- Máte na to **peníze** … Kolik vás to stálo, stojí a bude stát?
- Máte na to **čas** a **schopnosti** udržet krok s útočníky a bránit se efektivně a včas?

O2 IT Services

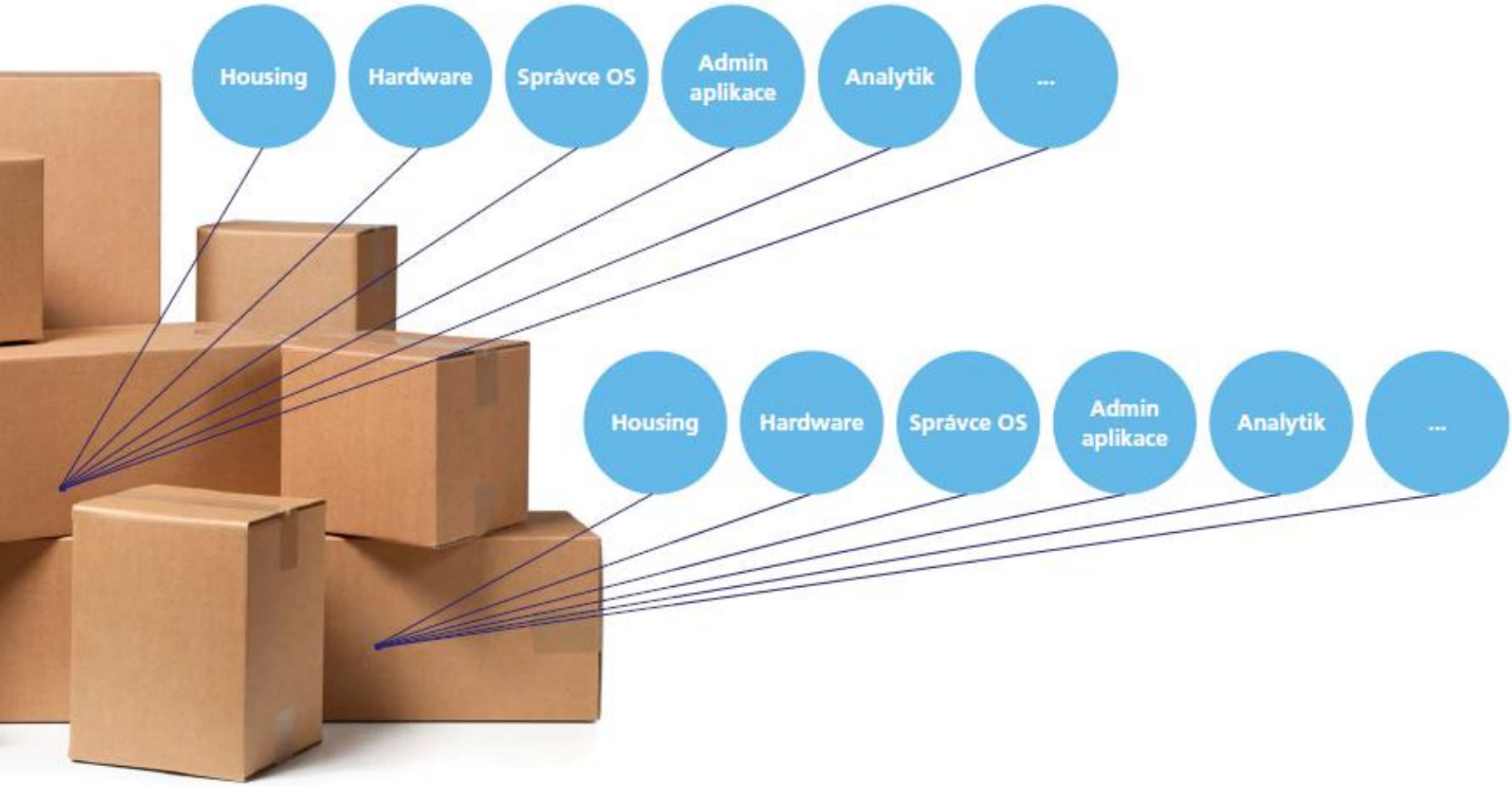
Jeden na to nestačí …..

Proces zajištění bezpečnosti IT



O2 IT Services

Krabice … jenom skladník to nevyřeší!



O2 IT Services

Průběh implementace řešení bezpečnosti IT

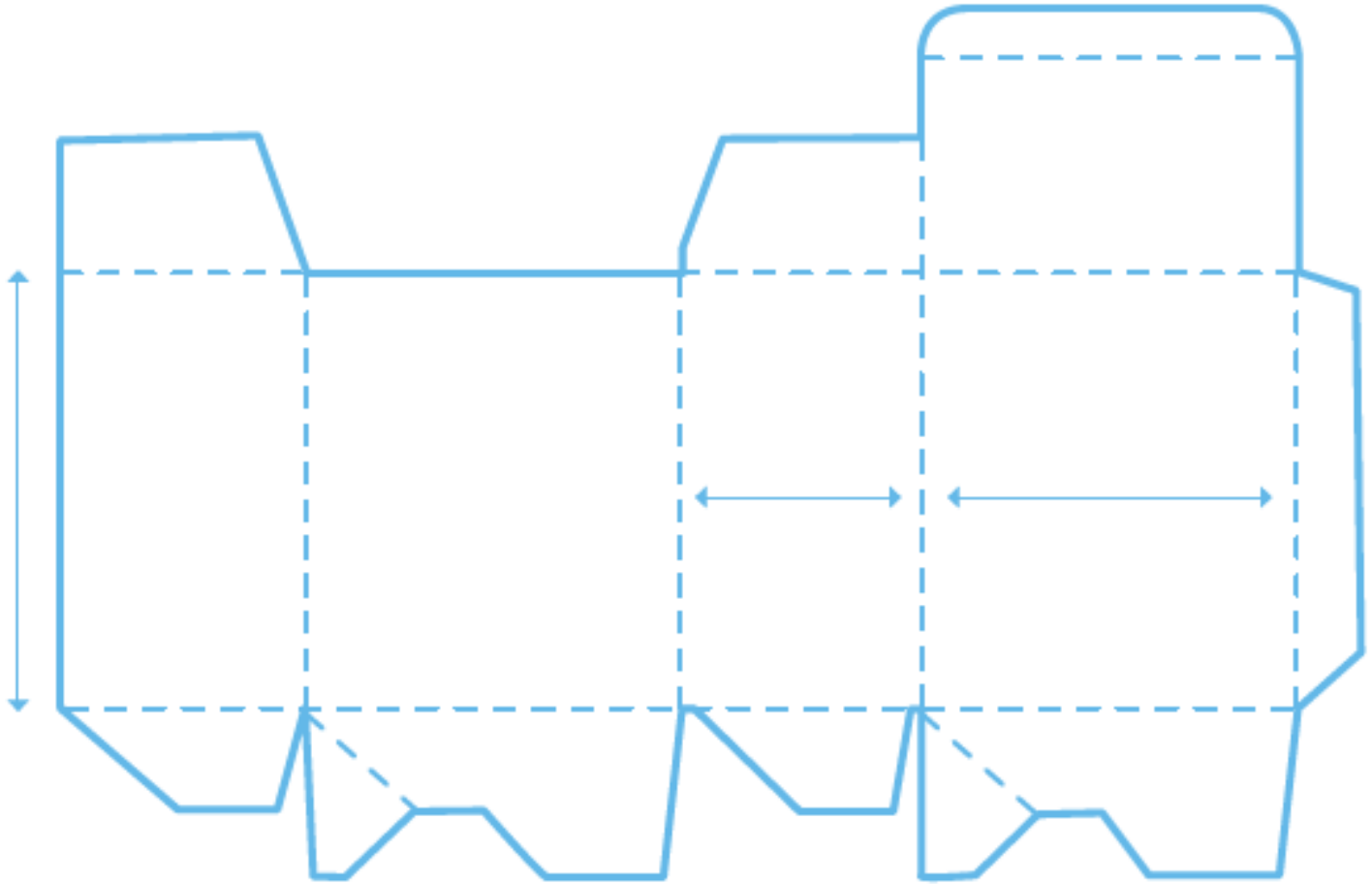
O2 IT Services

Máte dost času na …?

- Operativní řízení
- Taktické řízení
- Strategické řízení

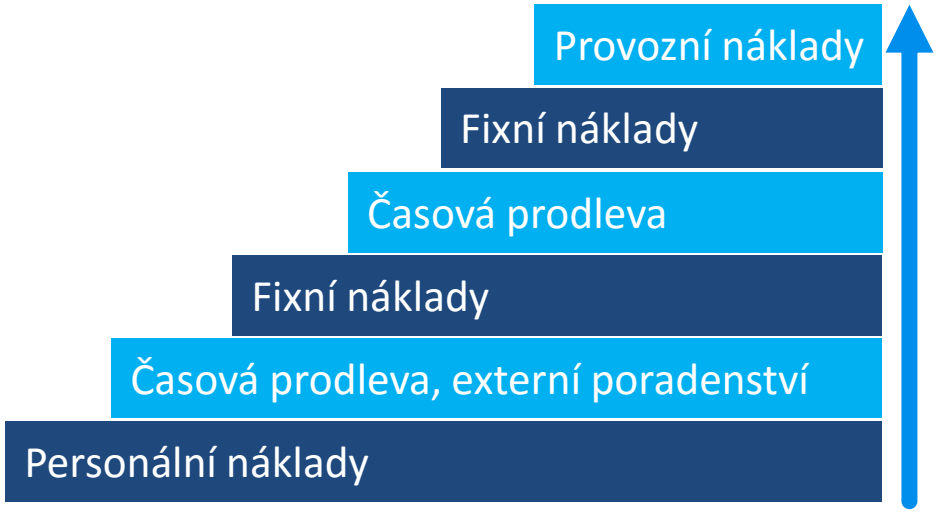
O2 IT Services

Chcete skládat krabice, nebo být skutečně chránění?

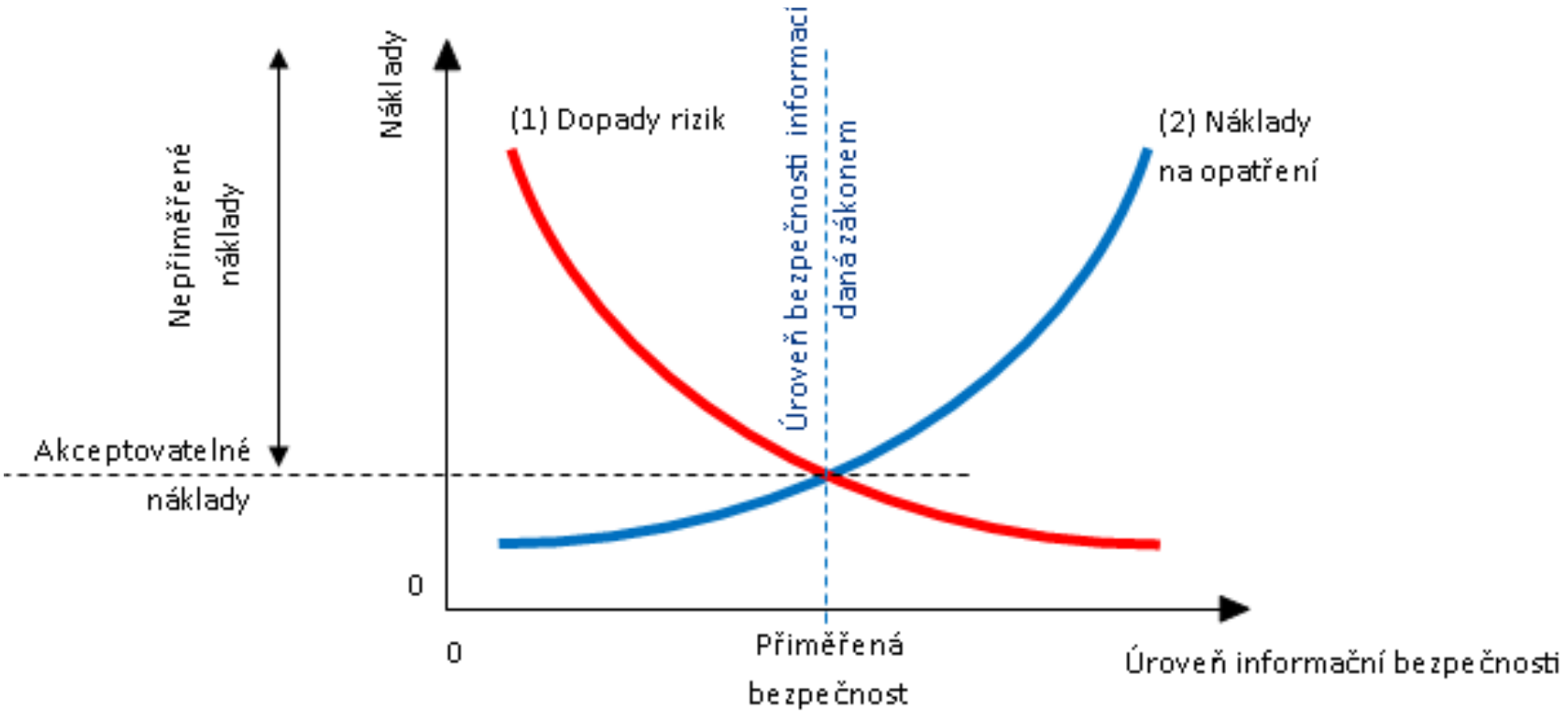


O2 IT Services

Vlastní zdroje, nebo raději službu?



Musíme to platit? Nepřiměřené náklady dle NBÚ



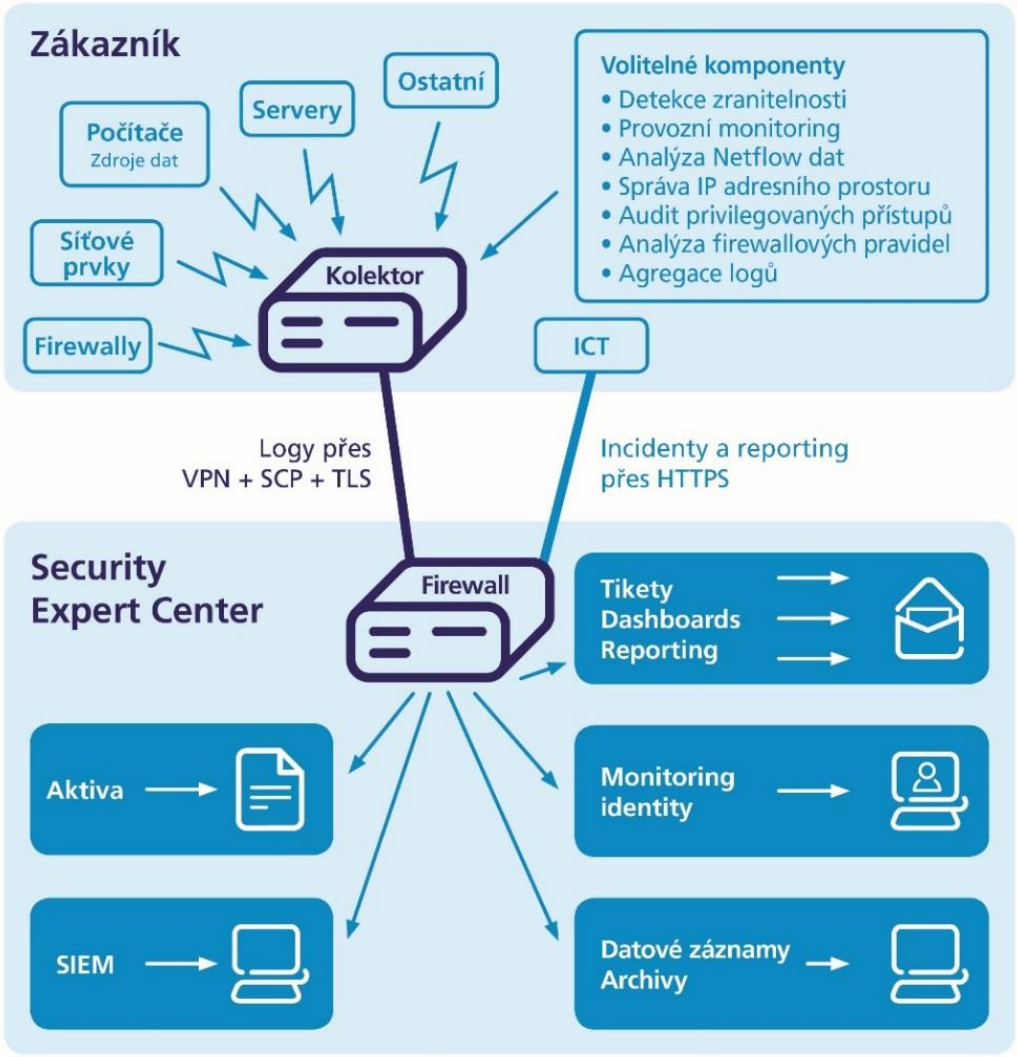
O2 IT Services

Služba Security Expert Center

- ✓ Pomáhá eliminovat kybernetická rizika
- ✓ Řešení kybernetické bezpečnosti vnímá jako **komplexní disciplínu**
- ✓ Identifikuje **klíčová aktiva** a nastavuje optimální model jejich ochrany
- ✓ **Modulární struktura** – monitoring, analýzy, reporting a další bezpečnostní služby
- ✓ Chrání **IT prostředí jako celek**

O2 IT Services

Součásti služby



Prevence

Detekce

Odpovědnost

O2 IT Services

Role SEC

SEC Operator (L1)

- Sleduje active channels a dashboards
- Vytváří anotace a cases
- Předává events a cases na SEC Analysts k dalšímu prošetření

SEC Analyst (L2)

- Prošetřuje incidenty s použitím active channels, grafů, anotací, cases a reportů
- Doporučuje a implementuje protiopatření

SEC Expert (L3)

- Identifikuje a navrhuje nové use cases
- Rozvíjí existující use cases
- Navrhuje a testuje nové korelace, filtry, monitory, aktivní listy, active channels, dasboards, reporty a trendy
- Rozšiřuje a doplňuje znalostní bázi a „Pattern Discovery profiles“

SEC Administrator

- Je zodpovědný za instalaci bezpečnostních komponent a za jejich správné fungování

O2 IT Services

Security Expert Center živě

Dotčené subjekty

Velké společnosti a organizace státní správy

Vlastníci kritické a významné infrastruktury

Společnosti se specifickými požadavky na bezpečnost informací

právní kanceláře, notáři, zdravotnická zařízení, finanční brokeři, novináři apod.

O2 IT Services

Případová studie 1

Security Expert Center pro kritické a významné systémy ve státní správě BOX 1

Klient
Organizace veřejné správy, která provozuje několik rozsáhlých agend s celostátní působností a současně informační systémy nezbytné pro svůj chod.

Požadavky
Systémy klienta byly klasifikovány jako kritické či významné a bylo třeba je uvést do souladu s požadavky zákona o kybernetické bezpečnosti a příslušných vyhlášek.

Prostředí
Systémové záznamy se v multiplatformním IT prostředí pouze shromažďovaly a ukládaly na lokální disky. Nevyužívaly se nástroje pro záznam aktivit uživatelů, neprobíhala detekce kybernetických bezpečnostních událostí a nebyl implementován ani nástroj pro ochranu před škodlivým kódem či sběr a vyhodnocení bezpečnostních událostí podle zákona o kybernetické bezpečnosti.

Řešení
V rámci správy záznamů byly nejprve instalovány dva kolektory pro záznam aktivit příslušných částí informačního systému klienta, jejich administrátorů a uživatelů. Záznamy se ukládají po dobu tří měsíců do důvěryhodného archivu a průběžně kontrolují analytiky SEC. Zjištěné bezpečnostně relevantní události a informace se odesílají do nástroje pro vyhodnocení kybernetických bezpečnostních událostí, který incidenty na základě pro zákazníka připravených a na doporučení analytiků neustále rozšiřovaných korelací automaticky vyhodnocuje. V rámci služeb SEC se v pravidelných intervalech uskutečňuje sken zranitelností a hrozeb. K detekci kybernetických bezpečnostních událostí, víceúrovňové ochraně před škodlivým kódem a filtraci internetového provozu mezi vnitřní a vnější sítí klienta se využívá služba O2 Next Generation Firewall. Byly rovněž nastaveny procesy zpracování a hlášení incidentů. Prostřednictvím webového rozhraní nezávislého tiketovacího systému jsou k dispozici informace o přístupech jednotlivých uživatelů do systému a k aktivům, o přístupech v rozporu s komunikačními a dalšími pravidly, o nejčastějších incidentech a s nimi spojených aktivech, o aktivech s největším počtem zranitelností a o řadě dalších.

Přínosy
Zatímco standardní implementace on-premise stejného rozsahu obvykle trvá několik měsíců, k přípravě, nastavení a kompletnímu uvedení služeb SEC do provozu stačilo pouhých šest týdnů. Požadavky zákona kybernetické bezpečnosti a souvisejících vyhlášek byly zcela naplněny a lze je navíc pružně rozšiřovat. Po celou dobu platnosti smlouvy má klient k dispozici profesionály SEC, kteří sledují aktuální stav bezpečnosti v organizaci a společně s analytiky reagují na vzniklé bezpečnostní hrozby v dohodnutém časovém intervalu. Náklady na bezpečnost se přesunuly z investičních do operativních.

Publikováno v Data Security Management 2016/1 (http://www.tate.cz/cz/casopis/clanek/dsm-2016-1-471/)

Případová studie 2

Bezpečnost při vývoji či změnách BOX 2

Klient
Začínající společnost, která vyvíjí aplikační bezpečnostní brány pro zabezpečenou komunikaci mezi přenosnými zařízeními, jako jsou mobilní telefony, tablety nebo zařízeních pro internet věcí, a aplikačními servery umístěnými u zákazníka.

Prostředí
Klient na platformě Linux v hostovaném prostředí datového centra O2 vyvíjí a provozuje kompletně nové a originální řešení bezpečnostních bran. Vývoj je navíc velmi rychlý, až překotný.

Požadavky
S velkým důrazem na pravidelnost a spolehlivost reportingu bylo třeba zajistit provozní a bezpečnostní dohled nově vyvíjených i provozovaných bran. K hlavním požadavkům patřily: sběr a ukládání systémových záznamů z provozovaných bezpečnostních bran, vyhodnocování kompromitovaných mobilních zařízení, možnost snadno připojit další brány umístěné kdekoli ve světě, nepřetržitý (24×7) provozní a bezpečnostní dohled v angličtině i češtině.

Řešení
Základem služby je správa systémových záznamů. Jejich sběr zajišťují dva kolektory umístěné přímo v datovém centru O2. Záznamy se uchovávají po dobu jednoho roku a slouží k vyhodnocování bezpečnostních událostí a incidentů. Součástí služby jsou nepřetržité bezpečnostní a provozní dohledy, nástroje pro tiketing a reporting. Byly rovněž navrženy konfigurace a dodán detailní návod na instalaci agentů pro sběr záznamů v již provozovaných nebo vyvíjených branách. Klient má k dispozici webové rozhraní pro komunikaci i různé způsoby upozorňování prostřednictvím tiketingu, e-mailu a SMS. Reporty jsou přizpůsobeny potřebám zadavatele. Obsahují např. výpis připojených mobilních zařízení a jejich přístupů, seznam kompromitovaných zařízení, přístupy k branám v rozporu se zadanými pravidly atd.

Přínosy
SEC velmi pružně řeší i překotné změny v zabezpečovaném systému a umožňuje na ně velmi rychle reagovat. Je dostupný celosvětově a nové bezpečnostní brány i další mobilní zařízení lze k systému připojovat jednoduše bez ohledu na jejich umístění. Konfigurace agentů pro správu záznamů zajišťuje plnou podporu všech systémů, i těch nově vyvíjených.

Publikováno v Data Security Management 2016/1
(http://www.tate.cz/cz/casopis/clanek/dsm-2016-1-471/)

O2 IT Services

Případová studie 3

Bezpečný informační systém obce BOX 3

Klient
Obec s rozšířenou působností, pro komunikaci s občany provozuje několik informačních systémů.

Prostředí
IT technologie na platformách Windows a Linux jsou umístěny v technologických místnostech. Správu zajišťuje minimální počet zaměstnanců s nulovým přehledem o aktivech organizace, která je třeba chránit. Systémové záznamy byly shromažďovány a ukládány pouze lokálně, chyběla základní bezpečnostní dokumentace.

Požadavky
Bez zásadních a nákladných úprav IT systémů obce a bez rozšiřování personálního zabezpečení jejich obsluhy bylo třeba zajistit bezpečnost IT provozu a služeb poskytovaných občanům.

Řešení a implementace
Bylo nezbytné identifikovat a klasifikovat aktiva organizace, vypracovat základní sady bezpečnostních dokumentů a na základě výsledků analýzy rizik realizovat služby sběru a ukládání záznamů pro Windows a Linux servery. Do prostředí zákazníka byly poté instalovány kolektory pro sběr záznamů. Záznamy se archivují po dobu tří měsíců a průběžně vyhodnocují analytiky SEC. Rozsah vyhodnocení je možné kdykoli rozšířit. Hlavním komunikačním kanálem klienta je webové rozhraní, k dispozici jsou i různé způsoby notifikace na základě zvolené úrovně upozorňování: tiket, e-mail a SMS.

Přínosy
Klient má k dispozici spolehlivou a účinnou službu, která řeší bezpečnost jeho informačních systémů a jimi poskytovaných služeb jako celek bez nutnosti pořizovat nákladné řešení on-premise a zaměstnávat další specialisty. Vytvořená dokumentace urychluje práci, určuje správné postupy a procesy a minimalizuje množství nejen procesních, ale i systémových a bezpečnostních chyb obsluhy. Pro řešení nenadálých nebo nepředvídaných situací je kdykoli k dispozici expertní tým SEC.

Publikováno v Data Security Management 2016/1
(http://www.tate.cz/cz/casopis/clanek/dsm-2016-1-471/)

O2 IT Services

Unikátnost Security Expert Center

Komplexní služba s vazbou na již používanou komunikační infrastrukturu

Dynamika: přizpůsobení aktuálním potřebám

Optimalizace nákladů: **OPEX**, nikoliv investice

Znalost klíčových aktiv s nastavením optimálního modelu jejich ochrany: **nový standard v bezpečnostních službách**

Naplnění požadavků **zákona o kybernetické bezpečnosti**

Snímá z beder operativu, uvolňuje ruce pro **strategii a taktiku**

Rychlost nasazení

O2 IT Services

Bezpečnost integrální součástí služeb

Zvýšení bezpečnosti služeb O_2

SEC je mandatorní a transparentní součástí

Stávající zákazníci

Noví zákazníci

Podpora bezpečnosti produktů / provozu

Individuální nastavení služby

Možnost volby

Bezpečnostní rámec O_2 IT Services

O_2 IT Services

Informační bezpečnost zajistí .....

Ochranu informací před hrozbami

Business kontinuitu společnosti

Minimalizaci finančních ztrát

Eliminaci reputačního rizika

Ochranu duševního vlastnictví

Nárůst obchodních příležitostí

Eliminaci ztráty zákazníků

Optimalizaci návratnosti investic

Ochranu před trestně-právní odpovědností

Přežití v businessu závisí na:

… dobrém nápadu, získání konkurenční výhody, agilnosti fungování

… a na jejich ochraně

O_2 IT Services

jiri.sedlak@o2its.cz

O2 IT Services