

**D A T A . . . . .**  
**S Y S**

**KYBERNETICKÁ BEZPEČNOST JE BOJ,  
ZVLÁDNETE HO SAMI?**

**RADIM PRACUCH**

+420 724 065 027 | [pracuch@datasys.cz](mailto:pracuch@datasys.cz)

# Rodinná firma

Realizujeme úspěšné projekty a spokojení  
zákazníci zůstávají s námi.



**MILOSLAV NOVÁK**  
*zakladatel společnosti*

**29 let chráníme  
Vaše DATA  
SYStematicky!**

**MARTIN NOVÁK**  
*CEO*



# Stačí pouze

# DOTACE?

## Stát chystá dotace na kyberbezpečnostní projekty, vyčlenil na ně miliardy

17. 8. 2022, 13:24 – Praha  
ČTK

Stát vyčlenil z evropských peněz na projekty zabývající se kyberbezpečností 3,4 miliardy korun. Ministerstvo pro místní rozvoj nyní spustilo první dotační výzvy, které mají pomoci se zabezpečením informačních a komunikačních systémů a zlepšením technické ochrany dat občanů. Informovalo o tom MMR.



## Kyberbezpečnost budou muset povinně zajistit tisíce českých firem

3. 9. 2022, 21:20 – Praha  
ČTK

Tisíce českých firem budou muset asi od poloviny října povinně zajistit kybernetickou bezpečnost. Počítá se s tím, že NIS2, jejíž konečný text by měl být znám v nejbližších dnech, bude mít 21 měsíců, aby ji zavedlo do své legislativy více organizací, které musí své počítačové systémy zabezpečit i dalšími subjekty. Za neplnění povinností jim hrozí pokuty.



## Veřejná i soukromá sféra. EU rozšiřuje požadavky na kybernetickou bezpečnost

28. 11. 2022, 14:04 – Brusel  
ČTK

Členské země Evropské unie v pondělí dokončily schvalování normy upravující požadavky ohledně úrovně kybernetické bezpečnosti ve firmách a ve státní správě. Směrnice rozšiřuje povinnosti na nové sektory včetně energetiky nebo zdravotnictví a má za cíl také zlepšit spolupráci příslušných národních orgánů. Na uvedení nových pravidel do praxe mají státy a zasažené podniky necelé dva roky.



# Proč uvažovat nově

Kybernetická bezpečnost si vyžaduje nepřetržitou pozornost

Doba si vyžaduje pokročilejší ochranu ICT aktiv.

Pro organizace to **přestává být zvládnutelné interními týmy.**

- Zvyšuje se sofistikovanost útoků a počet útočníků.
- Roste počet zranitelných míst – více IT, IoT, cloudů, home office ...
- Roste množství legislativních požadavků a regulací i oborových certifikací.

Také jste nainvestovali do bezpečnostních technologií a nestačí to?

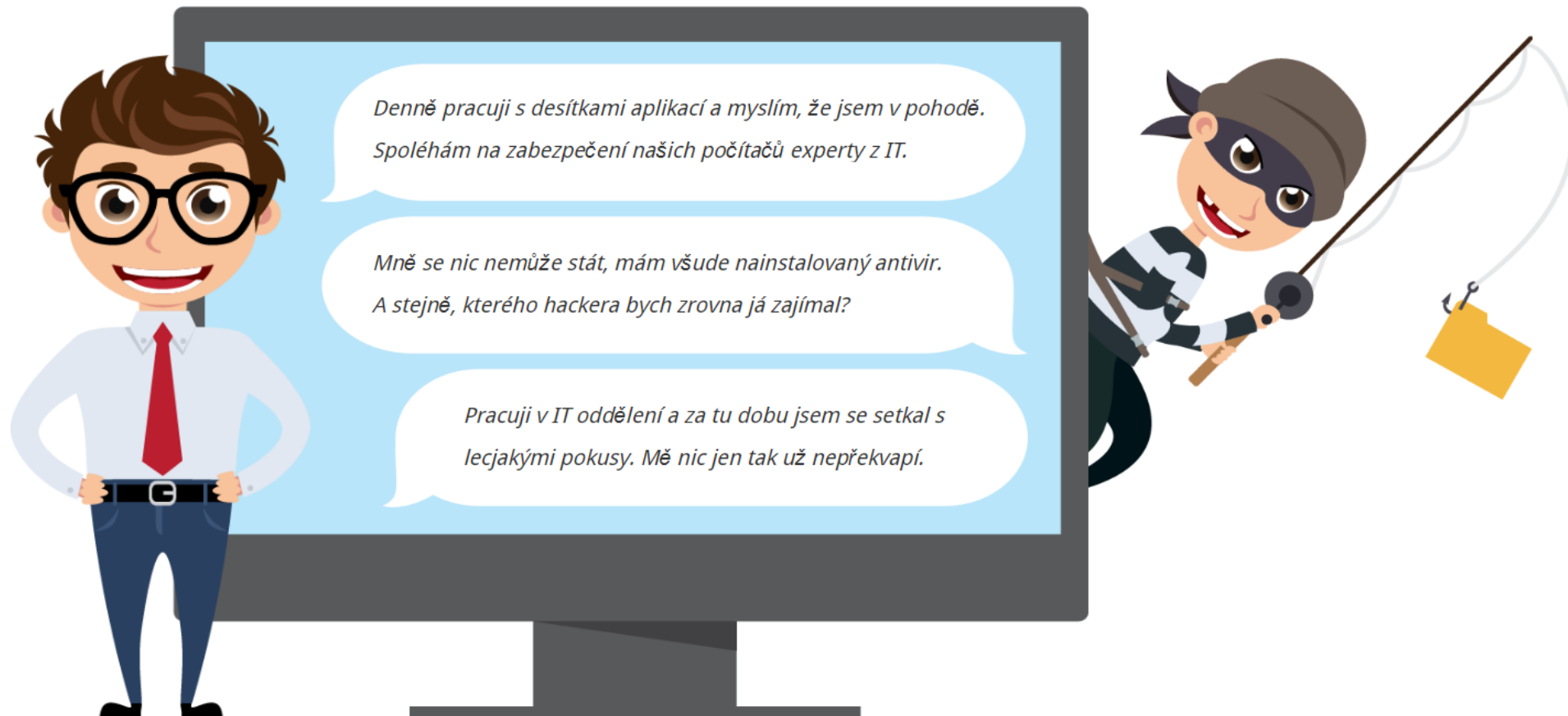
**TIP pro vás:** Porozumět potřebám a používat selský rozum.

- Začněte pečlivým určením toho, co potřebujete chránit.
- Využijte známý efekt 80/20 a usilujte o pevný řetěz.
- Neřešte za každou cenu vše interními týmy.
- Hledejte kreativní řešení s vysokou přidanou hodnotou a rychlým přínosem.



# Nečekejte na bezpečnostní incident, předcházejte mu!

TIP pro vás: Využijte Mikroslužby

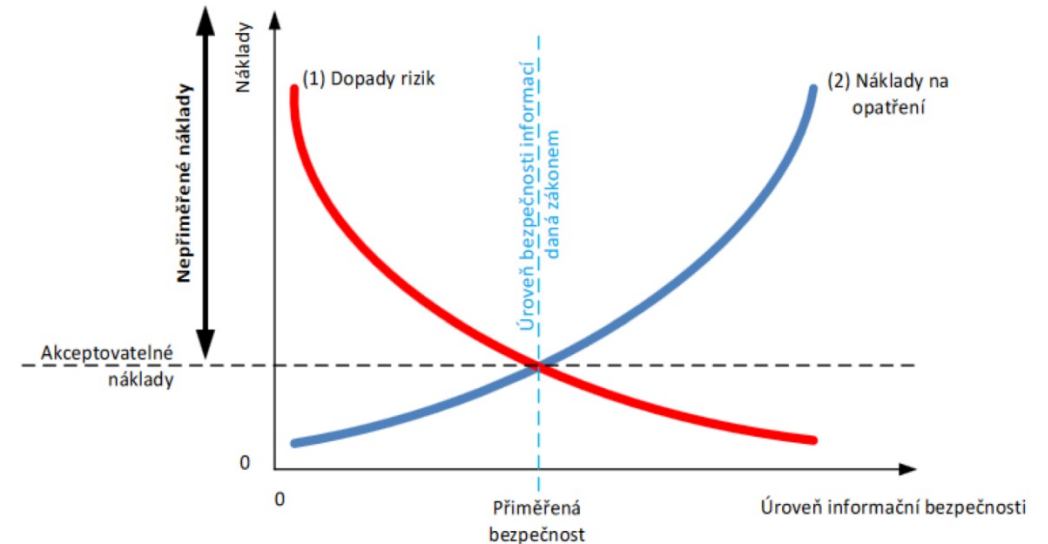


# Znáte své slabiny a rizika?

**Pro ochranu je důležité problémy vidět a vědět, a s jakou prioritou je odstranit.**

Poskytneme vám nástroje nebo službu, díky které jasně uvidíte, jak na tom jste a zkrátíte čas nápravných opatření. S realizací nápravných opatření Vám můžeme pomoci.

- Správa zranitelností.
- Školení vedení a zaměstnanců.
- Phishingové testy.
- Odolnost vůči ransomware.
- Testování výkonnosti a bezpečnosti sítě.
- Aktivní ochrana DNS provozu.
- Konfigurační rizika.
- Zhodnocení bezpečnostní reputace.
- Nezávislé posouzení nebo provedení testu obnovy zálohy, vč. návrhu technologií jak zajistit business kontinuitu
- Hardening



*Poskytneme vám nástroje nebo službu, díky které jasně uvidíte, jak na tom jste a zkrátíte čas nápravných opatření. S realizací nápravných opatření Vám navíc můžeme pomoci.*

# Stanovení rozsahu řízení kybernetické bezpečnosti

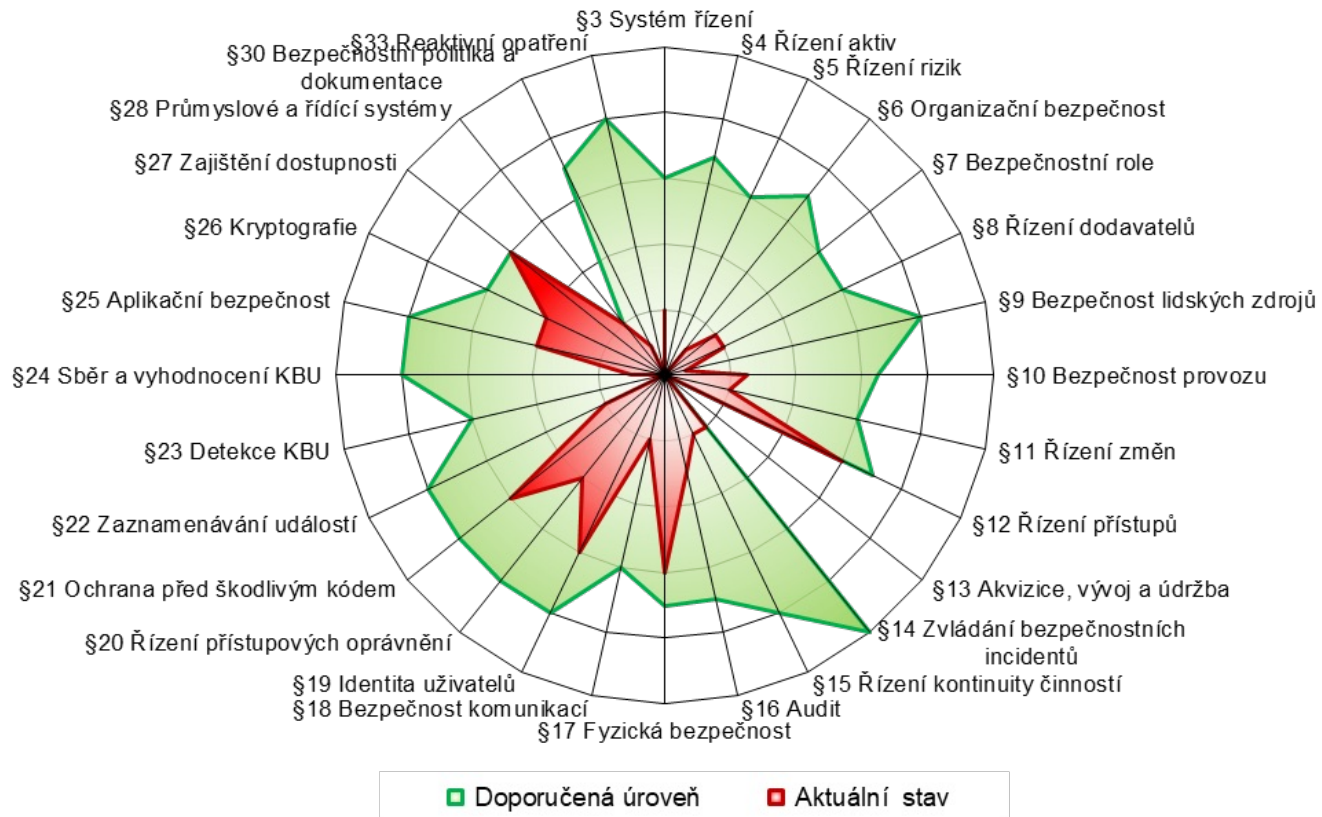
**Potřebujete vědět, co máte chránit.** Před implementací bezpečnostních opatření legislativa vyžaduje stanovit rozsah řízení kybernetické bezpečnosti, abychom určili aktiva spojená s poskytovanými službami, které mohou být vystavené kybernetickým rizikům.

1. Provedeme nezávislou analýzu současného stavu IT infrastruktury vaší společnosti a identifikujeme všechny důležité aktiva a procesy, které jsou zásadní pro fungování vaší organizace a poskytování služeb.
2. Během tohoto procesu mohou být také realizovány praktické testy (zranitelností, phishing, ransomware aj.), které mají za úkol zjistit reálný stav prostředí a služeb.
3. Součástí je také závěrečný workshop, kde budou diskutována konkrétní technická opatření na míru potřebám vaší organizace s cílem zvýšit úroveň kybernetické bezpečnosti.
4. Naším cílem je pomoci vám získat komplexní přehled o vaší organizaci a navrhnout opatření, která přispějí k vyšší úrovni kybernetické bezpečnosti.

## Přínosy:

- ✓ Posouzení požadavků zákona o kybernetické bezpečnosti a zajištění shody (GDPR, NIS2 atd.).
- ✓ Zpracování katalogu primárních a podpůrných aktiv.
- ✓ Mapování a analýza aktuálního stavu IT infrastruktury.
- ✓ Nezávislé hodnocení kybernetické bezpečnosti.

# Stanovení rozsahu řízení kybernetické bezpečnosti



## Zjištění z praxe:

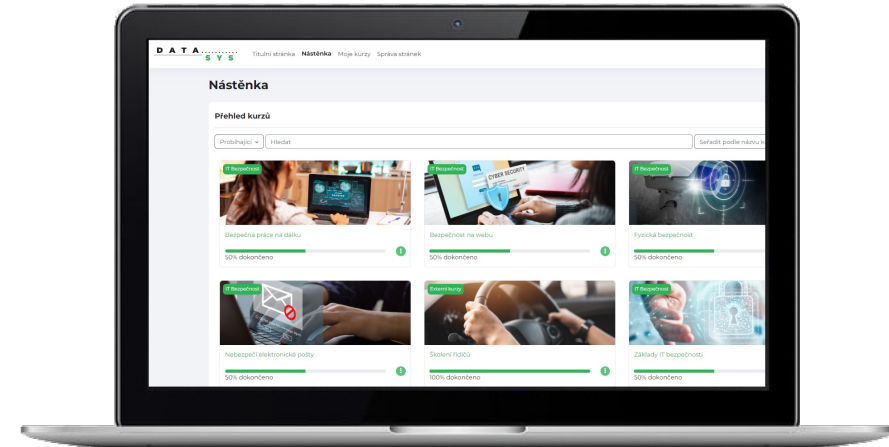
- Chybějící dokumentace a organizační opatření.
- Spoléhání se pouze na pečlivost a důslednost pracovníků IT oddělení.
- Nesoulad bezpečnostní politiky s realitou.

# Vzděláváte se?

**TIP pro vás:** Nejlepší odpovědí na bezpečnostní hrozby jsou poučení a odolní zaměstnanci!  
Školte je a průběžně prověřujte jejich znalosti.

## Využití e-learningu umožňuje

- dosáhnout značných časových a finančních úspor,
- vzdělávat zaměstnance kdykoliv a kdekoliv,
- snadné sdílení dovedností a zkušeností,
- jednoduché dodržování směrnic/nařízení,
- vytváření vlastního obsahu/kurzů.



**Ideální je kombinovat školení zaměstnanců a nasazení technologií pro jejich ochranu**

*Využijte námi dodávané e-learningové platformy i formou služby a našich vlastních kyberbezpečnostní kurzů.  
Pomůžeme Vám také se strategií přechodu na e-learning služby analýzou vzdělávacích potřeb.*

# Chybí vám lidé?

**TIP pro vás:** Kybernetická bezpečnost vyžaduje nepřetržitou pozornost!  
Doplňte svoje lidi zkušenými profesionály se zkušenostmi z jiných projektů.

Chybí Vám specialisté na kybernetickou bezpečnost?

Nemáte zkušenosti s identifikací a řešením incidentů?

Nemáte dostatek lidí na zajištění bezpečnosti nebo provozu v režimu 24x7x365 ?

## Zaveďte bezpečnostní dohled, nebo SOC

### Proč SOC službu?

Přestává být zvládnutelné a efektivní udržovat si vlastní týmy zaměstnanců s velmi specializovanými dovednostmi v oblasti sítí a kyberbezpečnosti?

Nabízíme unikátní koncept pružného aktivního bezpečnostního centra

eSOC, který se vám přizpůsobí.  [esoc.cz](https://esoc.cz)





Spolupracujme na bezpečnějšší budoucnosti.

Efektivní investice do správných bezpečnostních opatření jsou klíčem k úspěchu.

# Jaká bezpečnostní opatření zavádět

Preventivní kroky k posílení kybernetické bezpečnosti

## Okruhy bezpečnostních opatření

- Stanovení rozsahu kybernetické bezpečnosti.
- Politiky bezpečnosti informací.
- Kontinuita činností (tj. business kontinuita).
- Bezpečnost v rámci dodavatelského řetězce.
- Praktiky základní počítačové hygieny a vzdělávání v oblasti kybernetické bezpečnosti.
- Řízení přístupu a využívání vícefaktorového ověření identity, bezpečných komunikačních nástrojů.
- Řízení identit a jejich oprávnění
- Detekce a zaznamenávání kybernetických bezpečnostních událostí
- Řešení kybernetických bezpečnostních incidentů
- Bezpečnost komunikačních sítí
- Aplikační bezpečnost
- Kryptografické algoritmy

**Vedení má povinnost osobně absolvovat školení na téma kybernetické bezpečnosti a podporovat také své zaměstnance.**

# Národní plán obnovy 2023

Čerpání finančních prostředků na zajištění kybernetické bezpečnosti

## Podporované aktivity

- Audit kybernetické bezpečnosti
- Systém řízení bezpečnosti informací
- Zálohování a archivace
- Next-Generation Firewall vč. IPS/IDS
- Endpoint protection
- Load balancing
- Analýza a monitoring síťového provozu
- Multifaktorová autentizace
- Log management, SIEM a služby SOC
- Sandboxing
- Advanced Threat Protection
- Řízení přístupů a identit (PIM/PAM)
- Správa mobilních zařízení
- Správa aktiv a řízení rizik a zranitelností
- Servery a úložiště
- Kryptografický systém

**Oprávnění žadatelé**  
organizační složky  
státu kraje a obce

**Finanční rozsah  
projektů**  
5 - 300 milionů Kč  
v závislosti na typu  
žadatele

**Ukončení  
příjmu žádosti**  
prosinec 2024

# Důvěřují nám



Česká pošta



ŠKODA



# D A T A . . . . . S Y S

## **DATASYS - PRAHA**

Jeseniova 2829/20  
130 00 Praha 3  
tel.: +420 225 308 111  
e-mail: [datasys@datasys.cz](mailto:datasys@datasys.cz)

## **HRADEC KRÁLOVÉ**

Hořická 283/22  
500 02 Hradec Králové  
tel.: +420 225 308 640

## **PLZEŇ**

Schwarzova 50  
301 00 Plzeň  
tel.: +420 225 308 633

## **DĚČÍN**

Labská 694/24  
405 02 Děčín  
tel.: +420 225 308 250

## **OSTRAVA**

Vysoká škola báňská  
Technická univerzita Ostrava  
Studentská 6202/17  
708 33 Ostrava-Poruba  
tel: +420 724 065 027