Alternativní způsob řešení problému nedostatku odborníků kybernetické bezpečnosti

Mgr. Václav Pávek, MBA
Director, Global Delivery Services

Ing. Ondřej Tichý
Project Manager & Security Consultant

27.09.2022

CYBER SECURITY & NETWORK MANAGEMENT
HAS NEVER BEEN EASIER

Novicom – představení

- **Český výrobce řešení pro efektivní správu, monitoring a zabezpečení sítí**
- **Orientace na**
  - Střední a velké zákazníky
  - Zákazníky vyžadující vysokou míru bezpečnosti a provozní spolehlivosti svých sítí
- **Prosazuje na trhu přístup**
  - **Aktivního bezpečnostního dohledu - SOC**
- **Unikátní portfolio produktů a služeb využívající původní české technologie**
- **Prodej směruje výhradně do partnerské sítě v ČR i v zahraničí**

deník.cz

ZPRÁVY | PODNIKÁNÍ | SPORT | NÁZORY | MAGAZÍN | TIPY | MIMINKA | PRÁ

ČESKO | EVROPA PRO ČECHY | SVĚT | EKONOMIKA | REGIONY | KRIMI | KULTURA | ČEŠI V ČÍS

PŘEHLEDNĚ: Formulář pro opuštění okresu. Kde ho najdete, kam ho budete

Masivní kybernetický útok. Systém veřejné správy napadli ve čtvrtek hackeři

5.3.2021 | AKTUALIZOVÁNO 5.3.2021

ČTK

ČESKÝ ROZHLAS | RADIOŽURNÁL | PLUS | DVOJKA | VLTAVA | WAVE | ŽIVÉ VYSÍLÁNÍ | REGIONY | MUJROZHLAS | ESHOP

22. BŘEZNA 2021 | LEONA | 5°C, OBLAČNO

iROZHLAS

DOMOV | SVĚT | EKONOMIKA | SPORT | KULTURA | VĚDA | KOMENTÁŘE | ŽIVOTNÍ STYL | VOLBY | POČASÍ | VINOHRADS

ONLINE: Koronavirus ve světě a v Česku - čtěte aktuální zprávy →

Kde se nacházíte: iROZHLAS.cz / Zprávy z domova | Související témata: nemocnice hacker zdravotnické zařízení Česko Pavel Řezníček Evrop bezpečnost kybernetický útok koronavirus druhá vlna koronaviru koronavirus v Česku

Českou nemocnici opět napadli hackeři. Úřady jaké zařízení se jedná

Další českou nemocnici napadli hackeři. Podle kyberbezpečností společnosti Check Poi využili vyděračský virus ransomware a zašifrovali některé systémy zdravotnického za potvrdil i Národní úřad pro kybernetickou a informační bezpečnost. O jakou nemocnic nezveřejnily.

Praha 7:58 12. ledna 2021

iROZHLAS

DOMOV | SVĚT | EKONOMIKA | SPORT | KULTURA | VĚDA | KOMENTÁŘE | ŽIVOTNÍ STYL | VOLBY | POČASÍ

Sledujte válku na Ukrajině →

Kde se nacházíte: iROZHLAS.cz / Zprávy z domova | Související témata: Ředitelství silnic a dálnic Radek Mátl kybernetický útok Národní úřad pro

ŘSD se bude z kyberútoku vzpamatovávat n škody jsou velké, řekl šéf společnosti Radek

Ředitelství silnic a dálnic ČR (ŘSD) se bude z kybernetického útoku z minulého týdne vzpamatovávat několik měsíců, organizaci způsobil zásadní škody. V podcastu ŘSD to řekl generální ředitel organizace Radek Mátl. Podle něj šlo o propracovaný a dlouho připravovaný útok.

16:28 23. května 2022

ZPRÁVY

LUPA.cz

Lupa.cz » Články »

Kybernetický útok vyjde draho, prev vyplatí

ČT24

KOMUNÁLNÍ VOLBY | SENÁTNÍ VOLBY | RUSKÁ INVAZE | COVID-19 | DOMÁCÍ | SVĚT | RE

Obnova systémů ŘSD po kyberútoku stála desítky milionů. Brzy má opět fungovat i web s dopravními informacemi

28. 7. 2022

Do konce týdne spustí Ředitelství silnic a dálnic (ŘSD) web s dopravními informacemi, který je mimo provoz od květnového hackerského útoku. Generální ředitel organizace Radek Mátl uvedl, že náklady na obnovu systémů se vyšplhaly k 30 milionům korun, ale nemusí to být konečný účet.

Příběhy z historie českého internetu — Podcastový seriál

LUPA.cz

Rychlost Internetu | Články | Aktuality | Video | Podcast

Lupa.cz » Kyberútok zažívá každý týden na 1200 firem. Jak si hlídáte svou bezpečnost vy?

Kyberútok zažívá každý týden na 1200 firem. Jak si hlídáte svou bezpečnost vy?

PŘIDEJTE NÁZOR

REDAKCE | 2. 7. 2021

Aktuálně.cz

Sdílet článek | To se mi líbí

Kyberútoků na nemocnice je za dva měsíce skoro o polovinu víc, využívá se stavu nouze

deník.cz

ZPRÁVY | PODNIKÁNÍ | SPORT | NÁZORY | MAGAZÍN | TIPY | MIMINKA | PRÁCE

ČESKO | EVROPA PRO ČECHY | SVĚT | EKONOMIKA | REGIONY | KRIMI | KULTURA | ČEŠI V ČÍSLECH

PŘEHLEDNĚ: Formulář pro opuštění okresu. Kde ho najdete, kam ho budete potřeb

Další útok hackerů. Napadli systémy Správy železnic, provoz vlaků ale neohrozili

DNES 12:42

ČTK

Kybernetičtí útočníci v minulých dnech napadli počítačové systémy Správy železnic. Podle státní organizace však nijak provoz ani bezpečnost na tratích neohrozili. Případem se nyní zabývá Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB). Upozornil na to dnes Deník N. Hackeři útočili na sítě státních organizací i v minulých týdnech.

HOSPODÁŘSKÉ NOVINY

Na ochranu před kyberútoky nemáme peníze a stát nepomáhá, tvrdí rok šéfové nemocnic. Aktuálně hackeři útočili v Praze

LIDOVKY.CZ

NÝS | SPORT | KULTURA | CESTOVÁNÍ | RELAX | DESIGN | DOBRÁ CHUŤ | NÁZORY

020 20:07 | LIDOVKY.CZ > ZPRÁVY > SVĚT

ětší kybernetický útok v iách Spojených států. Hackeři povšimnutí několik měsíců vali citlivá data

ILUSTRAČNÍ SNÍMEK | FOTO: REUTERS

ox Až devět měsíců mohli počítačoví bez povšimnutí odčerpávat citlivé e z několika ministerstev. I když dné obvinění nepadlo, padá stín ní na Rusko. Napadení hlásí i firma t.

5 499 Kč

Aktuálně.cz

Sdílet článek | To se mi líbí

Branou pro útoky na úřady USA prý mohla být ruská firma sídlící v Česku. Ta to odmítá

rstock

19:53

řad pro vyšetřování (FBI) prověřuje, zda hackeři, kteří ých úřadů a firem, nepronikli také do softwaru ruské v Česku. S odkazem na své zdroje o tom informovala zpečnostní experti varují, že útoky, které trvaly

Novicom – pohled na oblast kybernetické bezpečnosti

Závažný globální problém

- **Nárůst počtu i závažnosti kybernetických incidentů**
- **Známé útoky v ČR**
  - ŘSD, Nemocnice Benešov, FN Ostrava, FN Brno, OKD, …
  - *Škody jsou ve výši stovek miliónů Kč*

Proč se to děje?

- **Podcenění managementem organizací**
  - není chápána závažnost problematiky
  - není ochota věnovat tomu adekvátní zdroje (finanční a lidské)
- **Kybernetická bezpečnost je svěřována přímo do IT oddělení**
  - IT je zaměřeno na zajištění provozu a za to je i hodnoceno
  - kybernetická bezpečnost odčerpává IT lidské zdroje a finance pro zajištění jejich primárního cíle

Novicom – pohled na oblast kybernetické bezpečnosti

- **Kybernetická bezpečnost dnes**
  - Zvyšuje se počet a závažnost útoků
  - Nemění se příliš vnímání managementu
- **Cybersecurity mají na starosti „ti naši IT-ci“**
  - kupují si kyberbezpečnostní hračky dle nejlepšího uvážení
  - často jim ale sami nerozumí a jejich využití zůstává za potenciálem přínosu
- **Management často nechápe nutnost věnovat se kybernetické ochraně systémově**
  - není dobře nastaven systém řízení kybernetické ochrany
  - nerozumí legislativním povinnostem a jejich důsledkům pro jejich organizaci

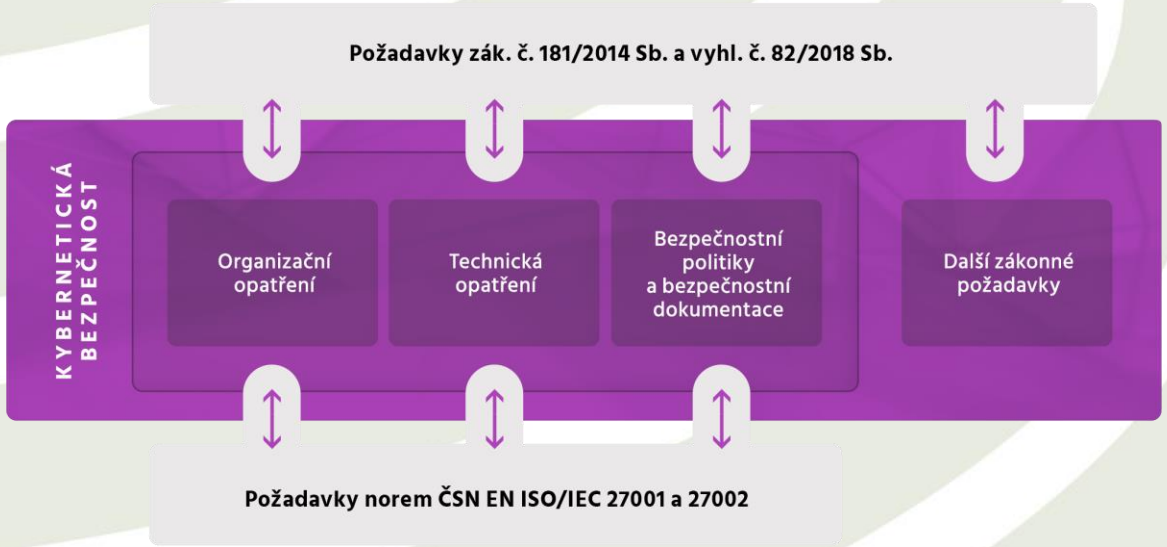
Novicom – pohled na oblast kybernetické bezpečnosti

- **Co mají části technické a organizační společného?**
  - Nejsou lidi…
  - Technickým řešením kybernetické ochrany pro 90%+ organizací je outsourcing klíčových částí nebo sdílení specialistů (aktivní bezpečnostní dohled – SOC)
  - Organizačním řešením nastavení systému řízení kybernetické bezpečnosti je kombinace technických nástrojů a outsourcing jinak nedostatkových specialistů
- **Mise Novicomu:**
  - Připravit organizace na připojení k aktivnímu bezpečnostnímu dohledu tak, aby byl schopen převzít zodpovědnost za výkon kyberbezpečnosti 24x7
  - Zajistit nastavení systému kybernetické bezpečnosti, aby byl plně v souladu s platnou legislativou a/nebo norem pro řízení kybernetické bezpečnosti

ADDNET BVS CCM APPLIANCE

Novicom CCM – Cybersecurity Compliance Management

- **Primárním cílem využití služby Novicom CCM je splnění legislativního souladu činnosti organizace v oblasti kybernetické bezpečnosti.**
- Novicom CCM je procesně-integrační platforma, která je pevně postavena na třech pilířích:
  - Vyspělá správa obsahu v souladu s EU a CZ legislativou
  - Automatizace a řízení procesů prostřednictvím nástrojů workflow
  - Otevřenost a snadná integrace



Novicom CCM = automatizace + dodržování zákonů + organizační bezpečnost

Novicom CCM – Cybersecurity Compliance Management

Vývoj legislativy v oblasti kybernetické bezpečnosti

- **Novela vyhlášky 317/2014 Sb., o VIS a jejich určujících kritériích** - významné rozšíření počtu dotčených orgánů a organizací
- **NIS 2 (Network and Information Security 2)** - směrnice Evropského parlamentu a Rady (EU)
  - rozšíření počtu povinných osob (odhad nejméně 6 000 soukromých i státních organizací)
  - zavedeno primární kritérium „velikost subjektu“ (není jediné kritérium)
  - postih: pokuta až 10 mil. EUR nebo 2% z celosvětového ročního obratu
  - pozastavení licence k poskytování služby, odebrání certifikace
  - v platnost cca v polovině roku 2024
- Lze očekávat novelu zákona č. 181/2014 Sb. a vyhlášky č. 82/2018 Sb.

Novicom CCM – Cybersecurity Compliance Management

- **Cloud služba** podpory činností manažera kybernetické bezpečnosti
- **Volitelně outsourcing výkonu** manažera, architekta a auditora kybernetické bezpečnosti
- **Cílem Novicom CCM je splnění požadavků platné legislativy** v oblasti kybernetické bezpečnosti - organizační opatření
- Speciálně **navrženo pro podporu činností manažera kybernetické bezpečnosti a týmu bezpečnosti**, který se podílí na zajištění kybernetické bezpečnosti významných informačních systémů a kritické informační infrastruktury
- Provádí **upgrade v závislosti na měnící se legislativě** a zajišťuje **uživatelskou podporu**

Novicom CCM – funkční rozsah

- Systém obsahuje vzorovou dokumentaci SŘBI dle přílohy č. 5 vyhl. č. 82/2018 Sb.
- Podpora pro komunikaci v rámci SŘBI mezi jednotlivými rolemi
- Jednoduchý registr aktiv (primárních, podpůrných i technických) a registr rizik, zranitelností a dopadů, nástroj pro tvorbu plánu zvládání rizik
- Hlídání termínů pro splnění povinností dle nastaveného kalendáře pro povinné úkony
- Distribuce úkolů jednotlivým rolím, včetně zajištění auditní stopy
- Základní proces řešení kybernetické bezpečnostní události/incidentu včetně formuláře pro reporting NUKIBu
- Podpora kontroly a auditu (využití vzorového dotazníku NUKIB a vazby na dokumentaci a procesy)
- Vzory základních dokumentů používaných v rámci systému (mimo předpisy) vč. vzorů pro podání NUKIB

Novicom CCM – služba pro koho a jak ji použít?

Komu je služba Novicom CCM primárně určena?

- Společnostem, orgánům a organizacím dotčeným ZoKB, tedy povinným osobám dle §3 ZoKB
- Správcům a provozovatelům VIS a KII
- Společnostem, které mají implementovaný SŘBI dle ISO/IEC 27001

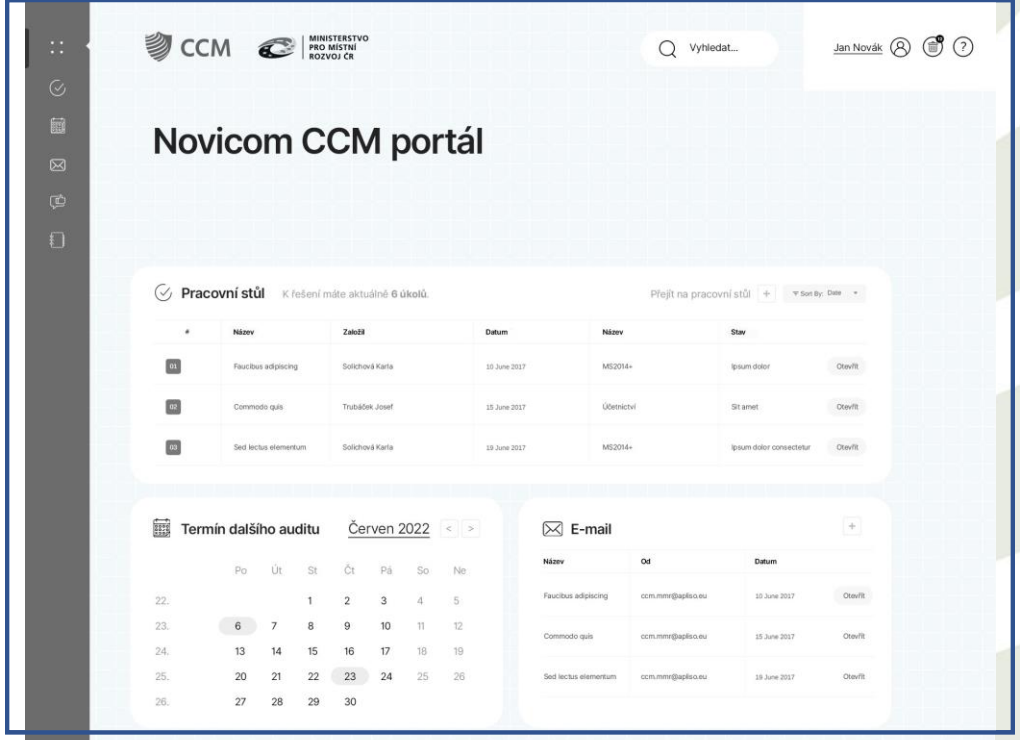
Novicom CCM je připraven na implementaci směrnice NIS 2

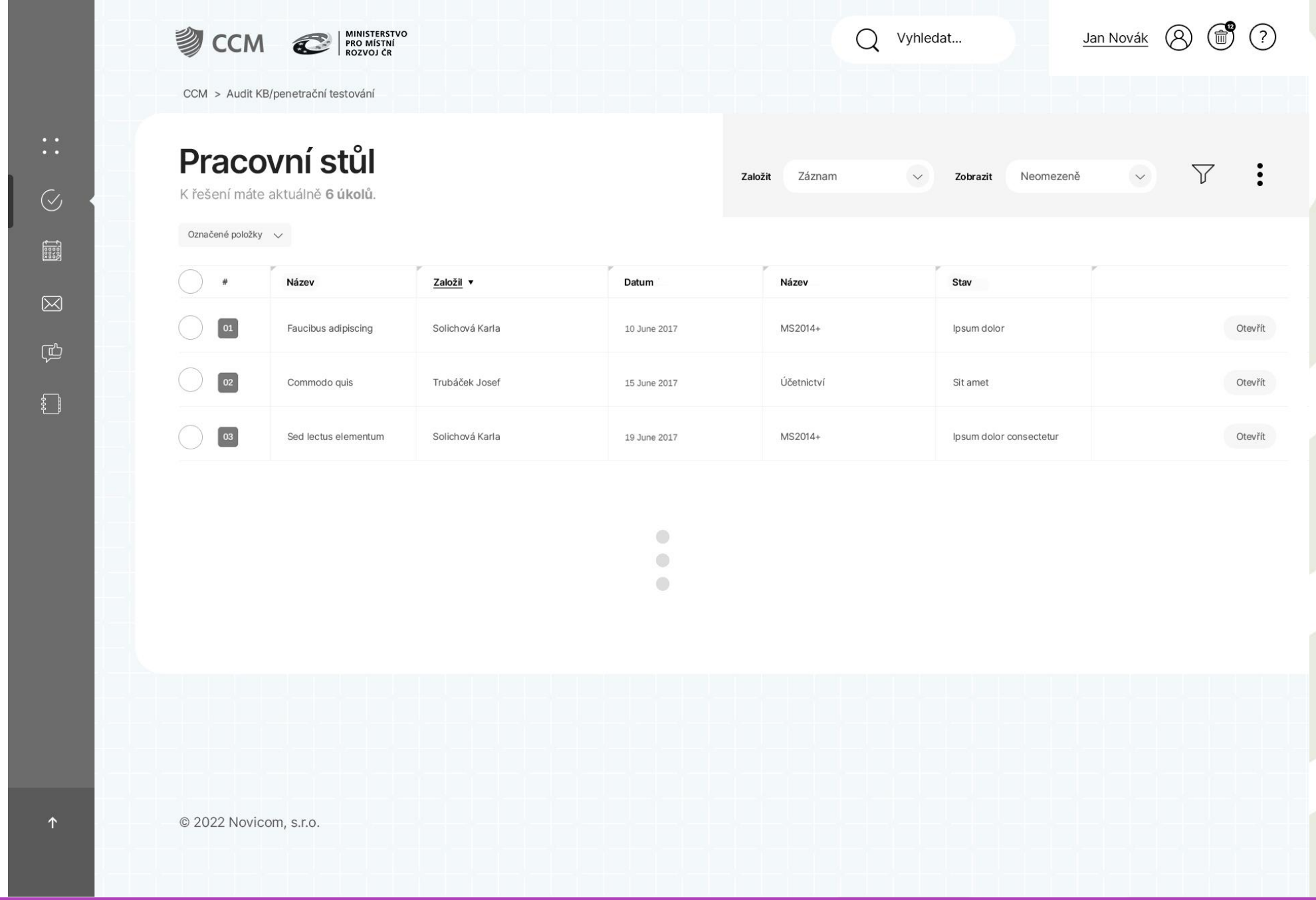
Jakým způsobem lze Novicom CCM použít?

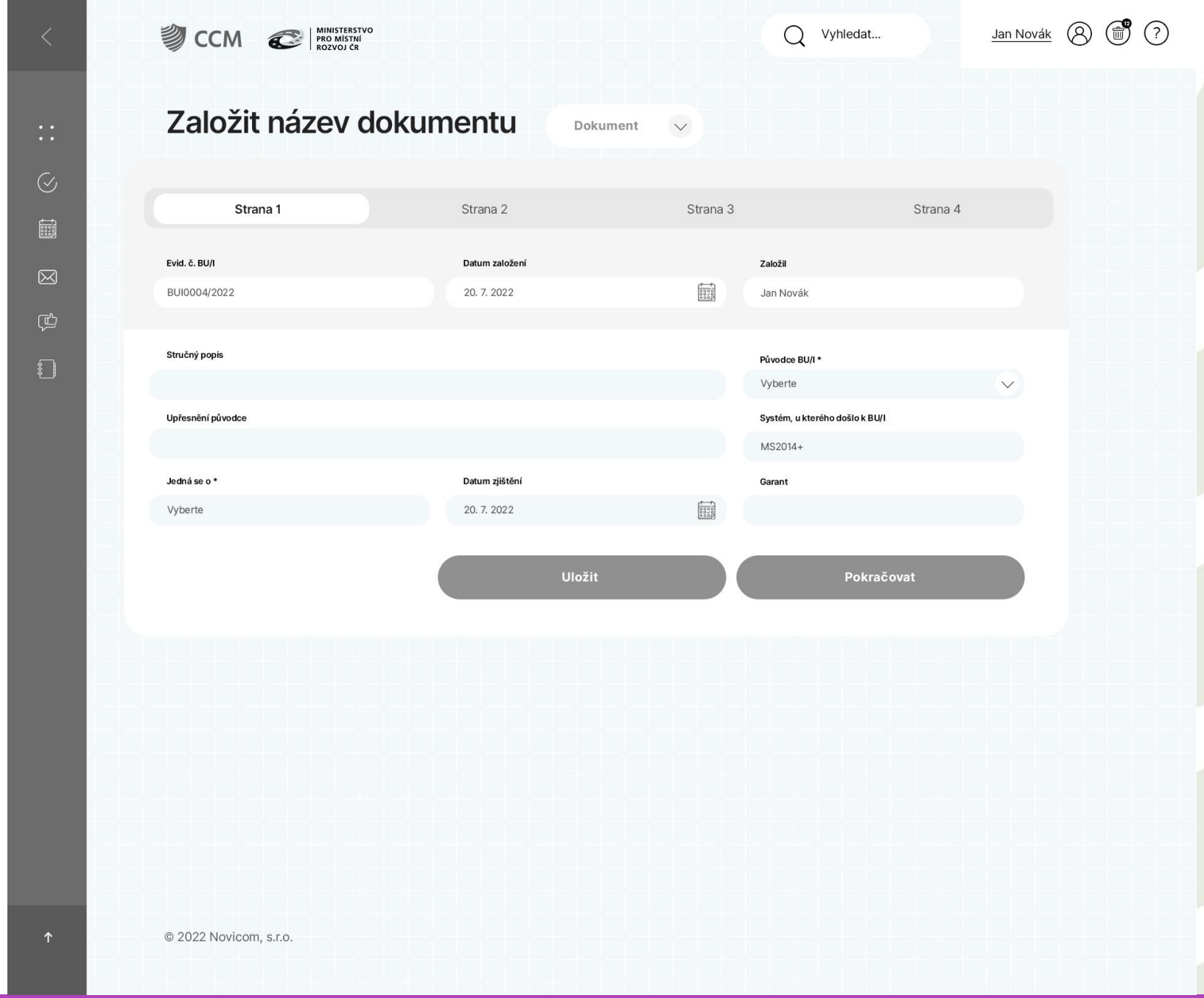
- On-premise
- Jako cloudovou služba

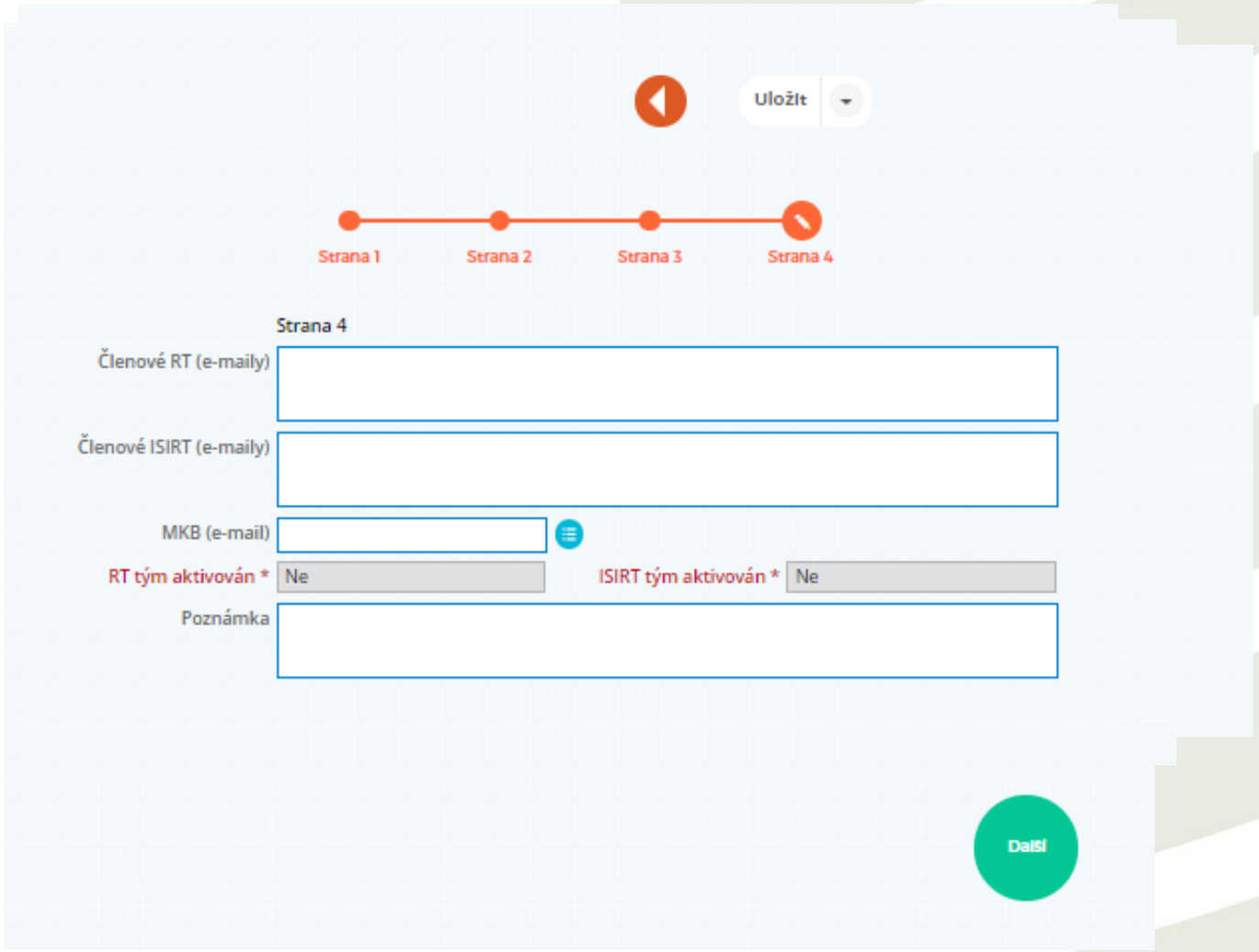
Novicom CCM – klíčové přínosy

- Jednoduchá webová aplikace
- Flexibilní cloudová platforma
- Zajištění dostupnosti, důvěrnosti a integrity uložených dokumentů díky využití robustní platformy Oracle
- Předpřipravené know-how (dokumenty a procesy) pro práci MKB
- Transparentnost a plný audit činnosti v systému
- Podpora organizace v případě krizových situací, díky předpřipraveným procesům (včetně eskalačních a komunikace s externími subjekty)
- Podpora týmové práce pracovníků, podílejících se na zajištění kybernetické bezpečnosti organizace
- Flexibilita při aplikaci legislativních změn v oblasti kybernetické bezpečnosti


CCM
MINISTERSTVO PRO MÍSTNÍ ROZVOJ ČR
Vyhledat...
Jan Novák
Novicom CCM portál
Pracovní stůl
K řešení máte aktuálně 6 úkolů.
Přejít na pracovní stůl
Sort By: Date
Název Založil Datum Název Stav
01 Faucibus adipiscing Solichová Karla 10 June 2017 MS2014+ Ipsum dolor Otevřít
02 Commodo quis Trubáček Josef 15 June 2017 Účetnictví Sit amet Otevřít
03 Sed lectus elementum Solichová Karla 19 June 2017 MS2014+ Ipsum dolor consectetur Otevřít
Termín dalšího auditu
Červen 2022
Po Út St Čt Pá So Ne
22. 1 2 3 4 5
23. 6 7 8 9 10 11 12
24. 13 14 15 16 17 18 19
25. 20 21 22 23 24 25 26
26. 27 28 29 30
E-mail
Název Od Datum
Faucibus adipiscing ccm.mmr@aplisa.eu 10 June 2017 Otevřít
Commodo quis ccm.mmr@aplisa.eu 15 June 2017 Otevřít
Sed lectus elementum ccm.mmr@aplisa.eu 19 June 2017 Otevřít
Předpisy a metodiky
Ut justo. Suspendisse potenti. Sed egestas, et vulputate volutpat, eros pede semper est.
Dokumentace 8
Báze znalostí 15
Legislativa 4
NÚKIB 0
Dokumentace pravidelné činnosti
Ut justo. Suspendisse potenti. Sed egestas, et vulputate volutpat, eros pede semper est.
Řízení událostí/incidentů 5
Audit KB / penetrační testování 3
Externí kontrola 0
Řídicí výbor kybernetické bezpečnosti 0
Řízení aktiv a rizik 3
Hodnocení dodavatelů 0
Opatření 0
© 2022 Novicom, s.r.o.


CCM
MINISTERSTVO PRO MÍSTNÍ ROZVOJ ČR
Vyhledat...
Jan Novák
CCM > Audit KB/penetrační testování
Pracovní stůl
K řešení máte aktuálně 6 úkolů.
Založit
Záznam
Zobrazit
Neomezeně
Označené položky
Název Založil Datum Název Stav
01 Faucibus adipiscing Solichová Karla 10 June 2017 MS2014+ Ipsum dolor Otevřít
02 Commodo quis Trubáček Josef 15 June 2017 Účetnictví Sit amet Otevřít
03 Sed lectus elementum Solichová Karla 19 June 2017 MS2014+ Ipsum dolor consectetur Otevřít
© 2022 Novicom, s.r.o.


CCM
MINISTERSTVO PRO MÍSTNÍ ROZVOJ ČR
Vyhledat...
Jan Novák
Založit název dokumentu
Dokument
Strana 1
Strana 2
Strana 3
Strana 4
Evid. č. BU/I
BUI0004/2022
Datum založení
20. 7. 2022
Založil
Jan Novák
Stručný popis
Původce BU/I *
Vyberte
Upřesnění původce
Systém, u kterého došlo k BU/I
MS2014+
Jedná se o *
Vyberte
Datum zjištění
20. 7. 2022
Garant
Uložit
Pokračovat
© 2022 Novicom, s.r.o.


Uložit
Strana 1
Strana 2
Strana 3
Strana 4
Strana 4
Členové RT (e-maily)
Členové ISIRT (e-maily)
MKB (e-mail)
RT tým aktivován *
Ne
ISIRT tým aktivován *
Ne
Poznámka
Další

Další informace o Novicomu?

Sledujte nás na:

- www.novicom.cz
- LinkedIn
- Facebook

Kontaktujte nás na:

- E-mail: sales@novicom.cz
- Tel.: +420 271 777 231

Adresa:

- Novostrašnická 176/39
- 100 00 Praha 10

novicom

CYBER SECURITY & NETWORK MANAGEMENT
HAS NEVER BEEN EASIER