HLAVNÍ MĚSTO PRAHA
Zastupitelstvo hlavního města Prahy

PID

Výbor pro IT a Smart City ZHMP

ZÁPIS z 27. jednání

Výboru pro IT a Smart City ZHMP konaného dne 2. 11. 2021 v 16.00 hod.

Videokonference

Přítomni: Mgr. Ing. Jaromír Beránek, Ing. Cyril Klepek, Bc. Jiří Koudelka, Ing. Jiří Kubíček, Ing. Ivan Pilný
Omluveni: Mgr. Zuzana Böhmová, Mgr. Radek Vondra, Pavel Zelenka,
Nepřítomni: Radomír Nepil, Mgr. Pavel Dobeš, Mgr. Zdeněk Zajíček
Tajemník: Ing. Renata Tomanová
Hosté: Mgr. Milan Hubka, Mgr. Ing. Zbyněk Loebl, Ing. Jiří Károly, RNDr. Rostislav Frys, Ing. Jan Petr, Ing. Martin Dušek
Jednání řídil: Mgr. Ing. Jaromír Beránek, předseda Výboru pro IT a Smart City ZHMP

Program:

Bod	Věc
1.	**Úvod**
2.	**Prezentace výstupů projektu "ePokuty: Využití metod umělé inteligence (AI) a online řešení sporů (ODR) pro optimalizaci výkonu agendy v oblasti řešení dopravních přestupků" - Milan Hubka, ředitel odboru dopravněsprávních činností MHMP a řešitelský tým projektu**
3.	**Představení systému pro detekci kybernetických hrozeb Fidelis Elevate, Jiří Károly, ředitel odboru INI**
4.	**Různé**

K jednotlivým bodům programu:

1. **Úvod**

Usnášeníschopnost Výboru:
Jednání bylo zahájeno za přítomnosti 5 členů Výboru z 11 celkem, vzhledem k počtu přítomných členů není Výbor usnášeníschopný, Výbor však nebude schvalovat žádná usnesení.

Volba ověřovatele zápisu: Ověřovatelem zápisu byl zvolen Jiří Koudelka jednomyslně.

Předseda Výboru J. Beránek přivítal přítomné na 27. jednání Výboru a představil plánovaný program.

Schválení programu jednání: program byl schválen.

2. **Prezentace výstupů projektu "ePokuty: popis stavu a návrh opatření“,** prezentuje Zdeněk Loebl, člen řešitelského týmu (detailně viz prezentace)

Z. Loebl: Jedná se o společný projekt advokátní kanceláře PRK Partners a Matematicko-fyzikální fakulty UK. Projekt je zatím ve třetině řešení. Děkuji panu řediteli Hubkovi a jeho odboru za spolupráci. Zefektivnění agendy lze docílit postupným přechodem na datově řízené online procesy jak ve vztahu k provozovatelům/ řidičům, tak interně. Na základě datové analýzy jsme dospěli ke zjištění, že většina přestupků nezaplacených před správním řízením je spáchána porušovateli opakovaně (systematicky).
Analyzovali jsme anonymizovanou databázi přestupků z let 2018, 2019, 2020. Na základě těchto čísel a za pomocí matematických modelů a teorie her předpokládáme zvýšení počtu uhrazených pokut. Zkoušíme zjednodušit současnou Výzvu k zaplacení pokuty a současně na web Pražana navrhujeme uvést otázky a odpovědi na časté dotazy. Navrhujeme bezpečný přístup (jedinečný kód nebo URL) k fotografiím případu, aby si dotyční mohli ověřit důkazy, dále způsob jak jednoduše a rychle určenou částku zaplatit. Na webu Pražana navrhujeme zpřístupnit jednoduchý uživatelsky přívětivý formulář k Podání vysvětlení, kde by adresáti Výzev mohli identifikovat řidiče, uvést že jejich SPZ je jiná než na fotkách, uvést že všechny fotky jsou rozmazané a nejde o jejich vůz, anebo jiné námitky.
Navrhujeme zavést informační linku pro etapu dopravní agendy – Výzvy za účelem informovat občany o webu Pražana, kde by měli podat vysvětlení online. Pro ty, kdo neumí online komunikovat, bude možnost reagovat poštou nebo sjednat schůzku s referentem.
V současnosti nejsou výzvy kategorizované. Proto navrhujeme zavést stejnou kategorizaci všech podezření na přestupek, jako již existuje ve správním řízení, např. rozšířením čísla Výzvy. Navrhujeme připravit dashboard společný pro členy obou týmů – pro Výzvy a pro správní řízení.
Výše uvedená opatření doporučujeme nejprve prodiskutovat interně na jednání se zástupci obou týmů (pro Výzvy a pro správní řízení), které proběhne v první půlce listopadu, následně vypracujeme návrhy obsahu dashboardu a provedeme uživatelské testování s pracovníky Magistrátu. Teprve poté, co uživatelské testování dopadne pozitivně, je možné odsouhlasená opatření začít implementovat. Toto bude práce pro příští rok.
V rámci opatření navrhujeme odstranit chyby Městské policie (např. nečitelná SPZ) i České pošty a to zpětnou vazbou, Policii ČR doporučujeme přejít na digitální komunikaci.
Bude záležet na magistrátu, zda výstupy na zlepšení této agendy využije nebo ne.

Diskuse:
I. Pilný: Kolik toto řešení bude stát a zda existuje business case, pro koho je určen?
Z. Loebl: Projekt je hrazen z prostředků TAČRu, naším úkolem je, aby správní řízení postupovalo rychle a efektivně, a aby způsob placení pokut byl pro občany jednodušší a přívětivější. Uživatelská fiktivní testování ukáží vypovídající výsledky. Ty budou zadarmo jak pro magistrát, tak pro městské části i obce v ČR.
J. Beránek: Souhlasím, že behavioralní analýza práva získává stále větší význam. Pokud se nabídnou lidem jednoduché cesty, jak mají splnit i nepříjemnou povinnost, tak potom může růst počet úspěšných vymáhání. Přínosem je také úspora zaměstnanců v odboru dopravněsprávních činností.
M. Hubka: Projekt se řeší v obecné rovině, aby ho mohl použít nejen magistrát, ale i městské části Prahy, popř. obecní úřady v rámci celé republiky. Zatím není žádný business plán, bude záležet na výsledcích a doporučení řešitelského týmu, která implementovat a která ne, za jakých okolnostech a výši financích.

M. Dušek: Jestliže budeme zatřiďovat a evidovat systematicky porušovatele, ptám se, zda na to máme oporu v zákoně? A zda je správné takto lidi kategorizovat?
Z. Loebl: My si myslíme, že četnost porušení je znakem závažnosti a závažnější přestupky by měly být trestány přísněji.
J. Beránek: Domnívám se, že to je i politické téma a měli bychom se o tom bavit v širší platformě. Myslím si, že na profesionální řidiče bychom měli klást vyšší požadavky na dodržování předpisů.
M. Hubka: Zákon s tím počítá. Výzva se posílá na každé oznámení o podezření přestupku. Ke stanovení výše pokuty je možné přistoupit dle závažnosti a recidivě, maximálně do výše dané zákonem. Ze zákona je povinné vést tzv. společné řízení o přestupcích, např. v případě překročení

deseti rychlostí, se vede jedno správní řízení a ukládá se jedna pokuta (jeden trest). Velké firmy mají přestupků hodně, např. leasingové firmy, které mají až tři tisíce aut, tak mají několik set přestupků denně. Pro zajímavost, vedli jsme řízení s provozovatelem o 300 přestupcích, rozhodnutí mělo 450 stran, ale mohli jsme uložit pouze 2 tisíce Kč.
J. Beránek: Souhlasím, že tento problém si žádá změnu legislativy.

J. Kubíček: Mám zkušenost s pokutami z Německa, výzvy byly formulovány srozumitelně česky, vystaveny automatem, a domnívám se, že je správné řešit obdobné případy automatizovaně, aby ubyla lidská práce. Cílem není jak pohodlně zaplatit pokutu, ale cílem má být, aby přestupků bylo co nejméně. Většina řidičů bere pokuty jako další dopravní daň, např. že nemohli zaparkovat.
Mám otázku na způsob zaplacení: nevím o tom, že by to bylo možné přes DS? Dále, zda existuje statistika platbou přes složenku? A jak je to se zasíláním hybridní poštou?
Z. Loebl: Ověřili jsme, že přes DS lze platit poplatky a pro MHMP by to mělo být zdarma.
M. Hubka: Rádi bychom, aby přestupků bylo minimálně, ale není tomu tak. Složenky jsme používali do r. 2004, lidé platí většinou online přes bankovní účty, ale jako jednu z možností ji necháváme. Výzvy k zaplacení určité částky zasíláme elektronicky do DS (pokud ji provozovatel má). Používáme tzv. hybridní poštu, což je služba České pošty, která přes DS od nás obdrží pdf dokument s naskenovaným podpisem, vloží jej do obálky a zašle. Dopisy online nelze použít pro orgány veřejné moci, ty jdou hromadnou konverzní poštou, spuštěnou od ledna t.r. Dokument se opět zasílá elektronicky s elektronickým podpisem do DS České pošty, která provádí úřední konverzi dokumentu, tzn. opatří ho konverzní doložkou, ochrannými znaky apod., vloží do obálky a zašle. Dokument odpovídá 1:1 originálu, elektronický dokument je zkonvertován na papírový. V rámci magistrátní spisové služby a České pošty probíhá testování a jedná se o smlouvě.
Z. Loebl: Opravuji, na slidu č. 8 má být uvedena hromadná konverzní pošta místo hybridní pošty.
Složenkami budou platit jen osoby, které nejsou počítačově gramotní, je to jen návrh.
J. Petr: Ke smlouvě s Českou poštou již probíhá připomínkovací kolo v TEDu.
J. Beránek: Jsem zastáncem toho, že se má občanům ulehčit způsob plateb v dnešní digitální době.

M. Dušek: V MČ Praha 14 probíhá pilot této konverzní pošty. Ještě k mé první poznámce – obávám se algoritmů, které se vytvářejí, aniž by byly stanoveny zákonem z pohledu státní správy.
Z. Loebl: Advokátní kancelář PRK byla vyhlášena právnickou firmou roku a jsme garantem legálnosti projektu.
M. Hubka: Pro nás je prioritou dodržování zákona. Nechceme nikoho kategorizovat, zákon s tím počítá s ohledem na četnost a závažnost přestupků. 26.11. připravujeme workshop, kde by řešitelský tým tohoto projektu představil jednotlivé výstupy z hlediska praxe, chceme na něj pozvat všechny zástupce MČ a tímto vás předběžně zvu, pozvánku zašlu prostřednictvím p. Beránka nebo paní tajemnice.

J. Beránek předal slovo řediteli odboru INI Ing. Károlymu

3. **Představení systému pro detekci kybernetických hrozeb Fidelis Elevate,** prezentuje Rostislav Frys (detailně viz prezentace):

J. Károly: Byli jsme požádáni p. ředitelem Petrem, abychom detailněji objasnili, co technologie Fidelis znamená a na co se používá. Magistrát má nakoupeny špičkové technologie a je třeba je dobře využít. V tomto spolupracujeme s českým Institutem robotiky a kybernetiky. Konzultant p. Frys vám podrobně technologii vysvětlí.
R. Frys: Fidelis je plně automatizovaná platforma k ochraně kybernetické bezpečnosti a je to nejlepší produkt z oblasti Security Operating Centre. Magistrát má mnoho dobrých technologií a teď je třeba, abychom dobře nastavili procesy, odpovědnosti, apod.
Fidelis Elevate aneb ADR (Automated Detection and Response) zajišťuje jistou část kybernetické bezpečnosti. Je především zaměřena na detekci a vyšetřování kybernetických incidentů, poskytuje komplexní pohled na dění v chráněném prostoru z hlediska kybernetické bezpečnosti, provádí

hloubkovou analýzu síťového provozu a zapisuje metadata. Zapisuje metadata i na koncových bodech (pracovní stanice, notebooky apod.), nesbírá uživatelská data, ale analyzuje důvěryhodnost spojení, certifikáty aj. Spojením všech těchto atributů získává komplexní pohled, kontext a automatizovanou analýzu dějů v síti z hlediska bezpečnosti, popř. reakci na kybernetické hrozby a události (incidenty), umí automatizovaně reagovat na kybernetické hrozby a události (incidenty).

Obsahuje tři základní moduly:

- **Fidelis Network** – detekce a prevence na síťovém provozu *(hloubková analýza síťového provozu)*
- **Fidelis Endpoint** – EDR – ochrana koncových bodů (detekce, reakce, remediace, vyšetřování)
  Spojením těchto dvou modulů vzniká XDR - Extended Detection and Response - je implementováno na MHMP
  To co, zatím není implementováno je
- **Fidelis Deception** – inteligentní pasti a návnady *(proaktivní „post-breach" detekce)*

Základní vlastnosti (schopnosti) systému Fidelis Elevate:

1. Protektivní – detekuje hrozby na síti a provádí ochranu úniku dat, současně detekuje hrozby/ události na koncových bodech
2. Reaktivní – na základě detekovaných hrozeb systém umí reagovat a současně částečně automaticky podporuje vyšetřování události
3. Proaktivní – provádí automatizované detekce hrozeb a reakce na události a již zmíněné „pastičky/ návnady" pro potenciální útočníky (zatím není zapnuto)

J. Károly: Zde doplním, že máme již připraveny tři POCéčka, jednáme o tom s naším dodavatelem, firmou Corpus a měly by být spuštěny do konce roku.
R. Frys: Ano, chceme si tyto funkcionality vyzkoušet v prostředí magistrátu a poté se rozhodne další postup.

4. Prediktivní – jde o oblast umělé inteligence, systém analyzuje nestandardní chování v daném prostředí, systém se sám učí a ví, jak vypadá běžný provoz organizace, hledá anomálie, porovnává je se vzorci chování, predikuje hrozby a události, které zatím nemá popsané ve své databázi.
5. Retrospektivní - automatizovaná retrospektivní analýza zkoumá, zda se objevily hrozby v průběhu posledních tří měsících a provádí příslušná opatření k opravě.

Pro provoz systém využívá hardwarové prostředky (servery a sondy) umístěné ve dvojici datových center magistrátu.
Systém je součástí komplexní architektury (slide 4), spolupracuje s preventivní ochranou koncových bodů, tj. antivir a ve spolupráci se softwarem Checkpoint (Harmony). Další část Fidelisu je síťová sonda, umístěna na vstupních bodech perimetru a na vstupech do intranetu a Mepnetu. Všechna data označená jako „alert", se sdružují do SIEM modulu, provádí se analýza Qradarem (produkt IBM) a SOC týmem analytiků, kteří analyzují reakce a reagují na případné incidenty.
Současně je Fidelis neustále zásobován novými informacemi o hrozbách, ty jsou rozesílány celosvětově a aktualizovány i v rámci naší instalace.
Analýza a statistiky provozu Fidelis Elevate - systém je po celou dobu provozu „laděn", bezpečnostní události jsou lépe filtrovány a jejich analýza je přesnější. V srpnu 2021 bylo zaznamenáno a vyšetřeno celkem 1 739 bezpečnostních událostí (stovky incidentů denně), tyto události jsou dále tříděny a vyhodnoceny.

Z hlediska analýzy provozu koncových bodů – je napojeno cca 2800 stanic a serverů, postupným upřesňováním detekčních pravidel jsou analyzovány jednotky až desítky událostí denně v provozu koncových stanic, např. 351 bezpečnostních událostí v květnu 2021.
Nejčastější detekce jsou: ransomware, komunikace na podezřelé IP, šifrovaná komunikace přes DNS, torrent, komunikace na CnC, pokus o zajištění persistence nežádoucího SW, vypnutí AV ochrany na koncové stanici, podezřelý soubor v systémovém adresáři, těžba kryptoměn, přenosy velkých archivů., Nobelium.

Nobelium, je příklad řešeného masivního kybernetického útoku, který proběhl na začátku července 2021. Jednalo se o celosvětový útok prostřednictví tzv. phishing techniky. Celkem bylo systémem Elevate zaznamenáno a zablokováno celkem 84 140 pokusů o aktivitu v rámci útoku. Útok byl dořešen a následně jsou nejen Fidelisem, ale také firewallem blokovány komunikace s CnC servery využitými k útoku NOBELIUM. Graf znázorňuje tisíce řešených incidentů denně v dané době, kdy útok probíhal. Na tom se ukazuje, že detekci incidentů není možné provádět pouze lidskými silami a že automatizace je zde na místě. Navíc systém pracuje v téměř reálném čase a systém se zablokuje v průběhu prvních pěti milisekundách.

Diskuse:

J. Kubíček: Probíhá v rámci srpnových 1739 bezpečnostních událostí další kategorizace, jaká byla příčina? Je někdo, kdo chtěl zaútočit zevnitř magistrátu? Existuje nějaká statistika uvedených 2800 koncových bodů, které fungují bezproblémově a naopak? Ladění a vyhodnocování incidentů je prováděno v rámci úřadu, anebo je proto využívána podpora dodavatele 14 MD měsíčně?

R. Frys: Ano, každá událost je došetřena, někdy automatizovaně. Všechny alerty jdou do SIEMu a do SOCu (Securite Operating Centre) a došetří se příčina. Příčiny nejsou koncové stanice, ale jsou na straně špatně zabezpečených serverech. Ale máme na tyto zranitelnosti pravidla a můžeme zareagovat. Vyhodnocování incidentů se provádí kombinací spolupráce se zaměstnanci magistrátu, osobami z vícero dodavatelů, osobami z Fidelisu a SIEMu, aby systém pracoval optimálně a 14 MD/ měsíc využíváme. Technologie pro detekci interních hrozeb připravujeme a budou nasazeny do konce roku a v 1. kvartálu 2022 vyhodnotíme jejich přínos.

M. Dušek: Mám dotaz, zda tento systém nezavádí nějaký vendor-lock co se týká síťových prvků?

R. Frys: Tento systém je zcela nezávislý na použitých technologií a nezavádí žádný vendor-lock.

M.Dušek: Kolik lidí je v SOC týmu? Jaké je jeho složení?

J. Károly: SOC tým zatím není plně sestaven, uvažujeme s podporou primátora o využití SOCu Letiště Praha a jsme v jednání. Pravděpodobně tým bude tvořen pouze outsourcingem. Aktuálně se jedná o bezpečnostní tým, který tvoří zaměstnanci z magistrátu z odborů INI a bezpečnosti, firma Corpus a SIEM nyní provozuje NGNs, kteří každý týden vyhodnocují incidenty. Pan Frys s námi spolupracuje na základě smlouvy s OICT.

M. Dušek: Jaký je další plán s nasazením do dalších částí Mepnetu, které se týkají MČ a MO?

J. Károly: Právě zítra se bude konat jednání ředitele MHMP s tajemníky všech MČ, já tam budu nabízet služby, které hlavní město městským částem může nabídnout. Tato služba zatím není v nabízeném katalogovém seznamu, jedná se spíše o delší budoucnost, a zda o to budou mít MČ zájem.

R. Frys: Prvním krokem je definování centrální politiky bezpečnosti z magistrátu, současně umožnit definování politiky bezpečnosti na lokální úrovni a toto propojit. Pracujeme na koncepci výhledově mít vše pod kontrolou.

M.Dušek: Vnímám to jako potřebný a dobrý krok.

J. Koudelka: Chtěl bych se zeptat na lidský prvek. Probíhají školení bezpečnosti zaměstnanců, jak se mají chovat a konkrétně reagovat? Existují pravidla bezpečnosti pro dodavatele softwarů a serverů?

J. Károly: Školení zaměstnanců není dostatečné. Standardy pro dodavatele aplikací a datových center existují, ale testovací prostředí správně nefunguje. Teď v listopadu před nasazením nové ostré verze GINISu proběhne testování s uživateli, které je lépe připraveno než v minulosti, ze které jsme se poučili.

R. Frys: Provedli jsme základní penetrační testy a revize přístupů na magistrátní servery, zavřeli jsme porty, které zůstaly otevřené v rámci nějakého testu, a při té příležitosti jsme prověřovali kteří dodavatelé mají přístup do sítě pomocí VPN a zjistili jsme, že jich je přes 60. Takže se velmi zpřísnila pravidla, povolují se individuálně za splnění přesně definovaných pravidel. Ale jsme asi jen ve čtvrtině procesu nastolení pravidel přístupu dodavatelů do infrastruktury.

J. Károly: Chceme úzce spolupracovat s Výborem pro kybernetickou bezpečnost, který by měl udávat směr. Např. jsme zjistili, že koncové počítače operačního střediska Městské policie jsou do internetu zapojeny pouze přes proxy server, což je pro nás dlouhodobé bezpečnostní riziko. Chce to také podporu z vyšších míst, aby se pravidla bezpečnosti takto neporušovala.

J. Kubíček: Většina útoků z internetu přichází z infikovaných subnetů. Správci jednotlivých sítí mají zájem dozvědět se, že z jejich sítě je prováděn nějaký útok a proto zřizují CSIRT týmy (Computer Security Incident Response Team). Je nějaká praxe, že by systém nahlásil detekci těmto týmům, aby mohli útoku zabránit.

R. Frys: Automatizovaně nikoliv, souvisí to s vyšetřením dané události. Jakmile je událost vyšetřena, tak po schválení ředitele J.Károlyho a odboru bezpečnosti tým informuje o incidentu patřičné účastníky. Většinou rovnou volám Kriminální policii na došetření veškerých stop.

J. Petr: Chci upřesnit, že školení ISMS zde probíhají, je součástí individuálního plánu vzdělávání zaměstnanců, jedná se o dvoudenní školení, poměrně kvalitní a ukončené testem.

J. Koudelka: Děkuji za otevřené odpovědi.

4. **Různé:** nikdo se nepřihlásil

J. Beránek: Příští jednání Výboru se bude konat 7. 12. 2021 od 16 hodin. Děkuji všem účastníkům, kteří se dnes připojili.

Jednání začalo v 16:00 a skončilo v 18:02.

Seznam příloh: 1. Prezentace ePokuty: popis stavu a návrh opatření.
2. Prezentace systému pro detekciJ. a vyšetřování kybernetických událostí Fidelis Elevate

Mgr. Ing. Jaromír Beránek
Předseda Výboru pro IT a Smart City ZHMP

Zapsala: Ing. Renata Tomanová, tajemnice Výboru
Ověřil: Ing. Jiří Koudelka