HLAVNÍ MĚSTO PRAHA
Zastupitelstvo hlavního města Prahy

PID

Výbor pro IT a Smart City ZHMP

ZÁPIS z 32. jednání

Výboru pro IT a Smart City ZHMP konaného dne 19. 4. 2022 v 16.00 hod.

Videokonference Webex

Přítomni: Mgr. Ing. Jaromír Beránek, Pavel Zelenka, Mgr. Zuzana Böhmová, Mgr. Pavel Dobeš, Ing. Jiří Kubíček, Bc. Jiří Koudelka; Ing. Ivan Pilný, Mgr. Radek Vondra,
Omluveni: Mgr. Zdeněk Zajíček, Jan Hušbauer
Nepřítomni: Ing. Cyril Klepek,
Tajemník: Ing. Renata Tomanová
Hosté: Bc. Ladislav Tobiáš, MSc., MPA (OICT MHMP), Jakub Karvánek, Viktor Jahna (oba Free Division)
Jednání řídil: Mgr. Ing. Jaromír Beránek, předseda Výboru pro IT a Smart City ZHMP

Program:

Bod	Věc
1.	**Úvod**
2.	**Data Governance – ochrana dat v prostředí MHMP**
3.	**Různé**

K jednotlivým bodům programu:

1. Úvod

Usnášeníschopnost Výboru:
Jednání bylo zahájeno v 16:05 h za přítomnosti 7 členů Výboru z 11 celkem, Výbor je usnášeníschopný.

Předseda Výboru J. Beránek přivítal přítomné na 32. jednání Výboru a představil plánovaný program.

Schválení programu jednání: program byl schválen jednomyslně.
Volba ověřovatele zápisu: Ověřovatelem zápisu byl zvolen Jiří Kubíček.

2. Data Governance – ochrana dat v prostředí MHMP – prezentují zástupci společnosti Free Division Jakub Karvánek (detailněji prezentace) a Viktor Jahna (ukázka SW Varonis).

L. Tobiáš: Pan primátor nás požádal o prezentaci a živou ukázku funkcí SW Varonis, který v prostředí MHMP používáme. V současnosti chystáme záměr do komise ICT na rozšíření licencí a nákupu nových modulů.

J. Karvánek: Naše společnost Free Division je oficiálním zástupcem výrobce softwaru pro Českou a Slovenskou republiku. Poskytujeme nadstandardní podporu zákazníkům a suplujeme tímto roli výrobce, nikoliv pouze prodejce.
Viktor Jahna je náš systémový inženýr a je jedním z nejlepších v Evropě. Podílel se na implementaci tohoto softwaru na MHMP, zná toto prostředí a předvede vám přímou ukázku systému.

Varonis spadá do oblasti tzv. Data Governance. Jedná se o zabezpečení dat z několika úhlů pohledu.
Pro zabezpečení dat platí obecně 4 základní kroky:
1. Identifikace a lokalizace citlivých dat z jejich celkového množství
2. Detekce - monitoring dat
3. Prevence - zajištění přístupových práv pro konkrétní uživatele
4. Udržitelnost – efektivní kontrolní mechanismy nesprávného toku dat

Klíčové vlastnosti Varonisu:
1/ ochrana nestrukturovaných dat
2/ splnění norem a zákonů z pohledu GDPR, zákona o kybernetické bezpečnosti aj.
3/ detekce hrozeb včetně reakce na ně
Výhodou je jedna centrální platforma a její implementace je v řádech člověkodní (MD). Varonis je schopen chránit data např. ve složkách odborů, SharePointů, MS Teams, Exchange, Active Directory a další a snižuje čas na detekci hrozeb až o 88 %. Varonis využívá mnoho subjektů v ČR i v zahraničí.

L. Tobiáš: pro MHMP hodláme rozšířit počet licencí (z 2000 na 3500), nakoupit nový modul, kde jsou předdefinována další pravidla, řešíme problém personální (pouze 1 osoba v odboru OIC), chceme zapojit odbor bezpečnosti a zmocněnkyni GDPR.

I. Pilný: Znamená to, že se se jedná o platformu Microsoftu a nejsou do toho zahrnuta data na Applu, na kterém pracuji? Monitoring dat se bude dotýkat i citlivých dat volených funkcionářů? Zatím to na mě působí jako „Velký bratr“, který vidí do všeho, ale kdo bude kontrolovat vás?

J. Karvánek: Varonis běží jen na serverových platformách, my nevidíme do počítače uživatele, ať už se jedná o PC či Mac/Apple. Varonis nesleduje obsah e-mailové schránky, něco jiného jsou přílohy.

L. Tobiáš: zastupitelské notebooky nejsou zahrnuty pod Active Directory, s výjimkou těch osob, které zastávají nějakou funkci, např. předsedové výborů ZHMP.

J. Karvánek: Varonis není „Velký bratr“. Data může sledovat jakýkoliv systém s určitým oprávněním. Zákazník si sám určuje, jaká práva, kdo má. Varonis je tzv. kukátko, které říká, kdo se na data podíval a co v těch datech je.
V. Jahna: Varonis leží na magistrátním úložišti, nikoliv na cloudu a já prostřednictvím VPN a smlouvy mám oprávnění k přístupu.

V. Jahna: Varonis sleduje nestrukturovaná data na serverech, nikoliv koncové stanice, sleduje všechny události s těmito daty a nyní vám ukážu simulaci řešení ransomwarového útoku.

V rámci prezentace proběhla diskuse – viz videozáznam určený pouze pro členy Výboru (0:35:35 – 1:19.37 a 1:24:08 – 1:26:11).

Dotazy:
J. Kubíček: Viděli jsme, že je tam 40 tis. citlivých dokumentů, které nemají vhodné oprávnění, ale domnívám se, že číslo je nadsazené kvůli obtížné detekci rodných čísel. Zaznamenal jsem, že zastupitelé nemají účet v Active Directory, ale neměli bychom být monitorováni kvůli korespondenci s občany, kteří mohou poskytovat rodná čísla.

J. Karvánek: Varonis nevidí do textu e-mailů, něco jiného jsou přílohy. U zastupitelů není Varonis nasazen pro Exchange a není to ani v plánu v jeho rozšíření.
J. Kubíček: Protože otevíráme přístup k dalším subjektům přes VPN, může být přístup k více dokumentům a je tu reálně možný další vektor útoků.
L. Tobiáš: Máte pravdu, v současnosti nám běží zakázka na privilegované účty.

J. Karvánek: Doplním, že účet p. Jahny a jeho VPN je pro zobrazení dat o datech, nikam dále. Varonis běží pod svým technickým účtem, jehož heslo by mělo být uložené v trezoru, na jiném místě než od jiných technických účtů, a vůbec se po počátečním nastavení se nepoužívá.

J. Karvánek: V rámci licence a po dobu fungování licencí má magistrát k dispozici tzv. bílý hackerský (white hackers) tým, který pomůže incident vyšetřit.

J. Koudelka: SW nástroj se mi líbí, je zajímavý a moderní. Kolik stojí provoz licence za rok? Jak se upravují pravidla ve Varonisu? Pravidla se aktualizují v návaznosti na útoky?

J. Karvánek: 165 pravidel jsou v základu Varonisu, cca 125 pravidel je tzv. strojově učících. Varonis si aktualizuje pravidla automaticky.
(Ukázka neobvyklého chování na ransomware-viz videozáznam od 1:28:36 – 1:32:00)

L. Tobiáš: Cena je kalkulována na 3 roky, za dokoupení licencí a modulů 2 950 tis./ rok, maintenance 2 600 tis./ rok, 30 MD na implementaci a 1 MD měsíčně na konzultační služby, provozní podpora činí 600 tis./rok. Kalkulace je na 3 roky.

J. Koudelka: Jak respektují pravidla úředníci, tzn. umísťování důležitých souborů odborů na sharepointech a ne na koncových stanicích.

L. Tobiáš: Soubory koncových stanic zaměstnanců leží také na serverech (home folder) a probíhá migrace dat do nových datových center.

J. Beránek: Jaký by měl být optimální postup, aby systém dobře fungoval?
J. Karvánek: dokoupit 1500 licencí na celkový počet 3500, rozšířit o modul Data Alert pro identifikaci útočníků, prodloužit případnou podporu a doporučujeme rozšířit o modul SharePointu. Závěrem bych chtěl zdůraznit, že Varonis podporuje všechny platformy, je to otevřený systém do budoucnosti.

J. Beránek: Děkuji vám za prezentaci, informace předáme členům komise IT.

3. **Různé:** Nikdo se nepřihlásil.

J. Beránek: Děkuji všem účastníkům, kteří se dnes připojili.
J. Koudelka se připojil 16:26
P. Dobeš se odpojil 16:31
I. Pilný se odpojil 17:30

Jednání začalo v 16:05 a skončilo v 17:40 h.

Seznam příloh: 1. Prezentace J. Karvánka

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

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