Meraki – System Manager / Cloud-Based Enterprise Mobility Management

1: Fakta – cíl zadavatele

Na základě požadavku zadavatele tento dokument (anonymizovaná verze zpracování z ledna 2015) plní tento cíl:

A) analyzovat Meraki – System Manager / Cloud-Based Enterprise Mobility Management (dále MSM) dle existujících zdrojů funkcionalitu MSM a prezentovat tuto laikovi srozumitelným způsobem (s uvedením zdrojů informací jak z veřejně dostupných, tak neveřejných – z archivů k této kauze získaných zdrojů)

B) popsat a prezentovat laikovi srozumitelným způsobem posouzení možných rizik úniku informací o provozu mobilních zařízení, provozovaných na mobilních sítích (od GSM, LTEC, přes WiFi po Cloud) i možné kompromitace jejich dat

C) dle zjištění ad b) výše prezentovat laikovi srozumitelným způsobem možné způsoby ověření reálného úniku informací o provozu mobilních zařízení, a kompromitace jejich dat

Zpracování odpovědí na otázky dle zadání vychází ze zadavatelem vedené konzultace a z veřejně dostupných zdrojů získaných podkladů – dokumentace MSM a návazných technologií.

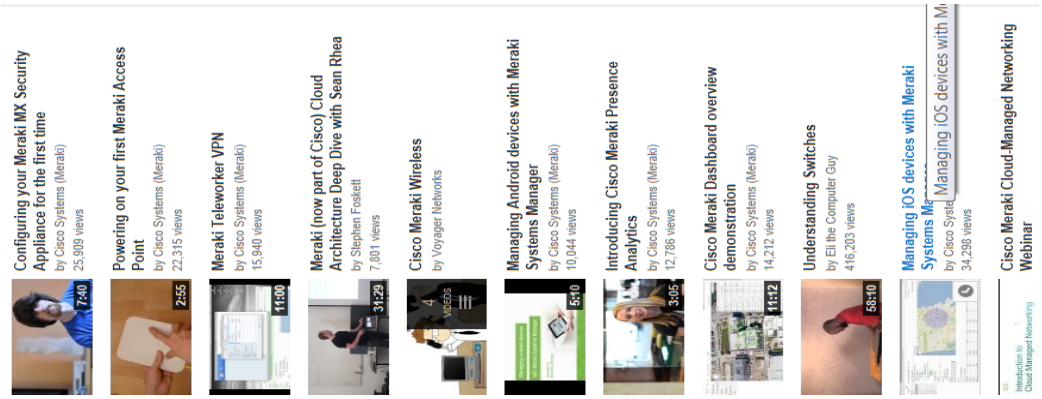
2: Vypracování – zjištěná fakta

Dle zadání byla zjištěna následující fakta k jednotlivým bodům zadání :

1 **ad bod a) zadání - analýza funkcionality produktu Meraki – System Manager / Cloud-Based Enterprise Mobility Management - je provedena takto :**

1.1 základní informace o MSM jsou získány z oficiálních zdrojů Meraki dle https://meraki.cisco.com/products/systems-manager

1.2 doprovodně pak hlubší informace čerpány z videoinstruktáží jak z z oficiálních zdrojů Meraki, tak také z https://www.youtube.com/watch?v=q4kwO4YlbJ4 např z násl uvedených :



1.3 Z výše uvedených zdrojů pak lze definovat základní funkcionalitu MSM takto :

1.3.1 MSM zajišťuje centrální správu (tj. řízení) , diagnostiku, monitorování a zabezpečení mobilních zařízení uživatelů (mobily, tablety, notebooky), a to prostřednictvím bezdrátové, na přístupu k Meraki Cloud (pozn. – výraz „cloud“ tj. oblak se do češtiny nepřekládá, je to datový prostor na síti internet pro sdílení dat, aplikací služeb aj.) založené technologii.

1.3.2 MSM tímto pak dále prostřednictvím cloud umožňuje :
- lokalizovat zařízení uživatelů dle zařízeními v GPS poskytovaných dat
- instalovat na dálku do zařízení uživatelů programy
- doručovat na dálku do zařízení uživatelů data
- provádět na dálku v zařízení uživatele změny bezpečnostní politiky daném zařízení , a to až do úrovně zrušení přístupového kódu (tj. hesla pro odemčení zařízení před neoprávněnými uživateli), či zablokování zařízení, nebo vymazání veškerých dat v zařízení,
- provádět na dálku nastavení zařízení uživatele od přístupu k sítím (GSM, WiFi aj.), vypnutí, restart i zálohování dat
- provádět na dálku v zařízení uživatele jeho diagnostiku vč. vyhledávání chybových stavů

1.3.3 MSM je multi-platformní prostředí, tj. výše uvedenou funkcionalitu je schopen provádět v prostředí všech hlavních výrobců informačních technologií (dále IT), tj. :

- Apple a jeho zařízení s operačním systémem (OS) s názvem iOS,
- Microsoft s OS Windows,
- se zařízeními výrobců, užívajících systém Android.

1.3.4 MSM je prostředí, které funguje nezávisle na lokalitě daného zařízení, tj. funguje kdekoli na světě, MSM není závislý na připojení k internetu, tj. funguje také bez připojení ovládaného zařízení k Internetu.

DÍLČÍ ZÁVĚR K BODU A/ ZADÁNÍ

Z hlediska zde popsaných vlastností MSM je vidno, že tento produkt efektivně soustřeďuje téměř veškerou funkcionalitu, potřebnou pro IT profesionály pro správu, řízení diagnostiku i ochranu firemních mobilních technologií s cílem udržet tyto mobilní prostředky uživatelů v provozu s minimálním rizikem výpadku jejich funkčnosti či dokonce kompromitace jejich provozu, dat či uživatele. Z tohoto pohledu je proto MSM pro IT profesionály, zodpovídající za správu, řízení diagnostiku i ochranu firemních mobilních technologií nezbytným prostředkem pro jejich účinnou a efektivní práci.

Nicméně takto široce pojatá funkcionalita, jakou nabízí MSM s sebou nese také provozní i bezpečnostní rizika, které je nutno řešit již při přípravě nasazení produktů této kategorie, tj. jak v projektové fázi, kdy je nutno recipročně k produktem nabízené funkcionalitě vnímat též možná ohrožení funkčnosti zařízení či dokonce kompromitace provozu, dat či uživatele, a to jak vlivem lidského činitele – osobami správců, přistupujících k aplikacím typu MSM, tak vlivem nedostatečné úrovně bezpečnostních standardů pro provoz aplikací typu MSM.

Podcenění či dokonce nedostatečné vyhodnocení rizik v projektové fázi může pak přinést v provozní fázi nasazení produktů typu MSM rizika nedostatečného fungování zařízení uživatelů spravovaných prostřednictvím MSM, případně též rizika nepředvídatelných výpadků zařízení, či dokonce riziko kompromitace provozu, dat či uživatele zařízení.

Je proto nanejvýš potřebné znát pro posouzení nasazení a provoz prostředků typu MSM veškeré informace (např. Studie proveditelnosti, Předprojektová analýza rizik, Projekt nasazení, provozní předpisy typu Bezpečnostní politika a systém kontrol provozovaného nasazení aj.) které vedly k jeho projektování a nasazení, a to v odborné, tak i v legislativně právní rovině, toto vše vč. kompetencí a zodpovědnosti autorů, schvalovatelů i realizátorů uvedeného projektu ve fázích od jeho přípravy, schválení, nasazení do zkušebního provozu i v jeho vlastním rutinním provozování.

2 **ad bod B) zadání – posouzení možných rizik úniku informací o provozu mobilních zařízení, provozovaných na mobilních sítích i možné kompromitace jejich dat - je provedena takto :**

Jak vyplývá z Analýzy funkcionality MSM provedené pod podem A) zadání, existuje v tomto případě značné riziko úniku informací o provozu mobilních zařízení, provozovaných na mobilních sítích i možné kompromitace jejich dat, a to zejména pokud není celý projekt nasazení MSM řádně veden jak po odborné, tak po legislativně - právní úrovni.

Tento dokument nehodnotí projekt po legislativně – právní stránce, proto se v dalším bude zabývat pouze věcně – odbornou a provozní stránkou nasazení MSM, a to z hlediska běžné praxe IT.

Jak již naznačeno v dílčím závěru k bodu A) výše, rizika úniku informací o provozu zařízení na mobilních sítích (dále jen mobily) i možné kompromitace jejich dat, jsou zejména následující :

2.1 ohrožení prostřednictvím lidského činitele – správců i jiných pracovníků dohlížejících na provoz aplikace MSM, kteří mají k MSM a jeho členům – mobilům uživatelů – nejvyšší možná práva v celé šíři funkcionality ad bod A) tohoto ZP, z těchto práv pak vyplývají zejm. následující :

2.1.1 úplné odstavení mobilu uživatele z provozu, výmaz jeho aplikací i dat,

2.1.2 ztráta databáze mobilu i historie jeho komunikace (hovory, vš. druhy zpráv, maily, geo data aj.)

2.1.3 porušení osobnostních práv uživatele mobilu ve vztahu k jeho osobním aktivitám a údajům (sledování – lokalizace pohybu uživatele v prostoru a čase, monitorování jeho komunikace)

2.1.4 kompromitace uživatelem nastavených hesel (riziko průniku těmito hesly i do jiných zařízení či osobních prostředků uživatele – zabezp. systémy privátního majetku aj.)

2.1.5 možnost převzetí uživatelem mobilu řízených aktivit – od řízení bezpečnosti až po převzetí komunikace mobilu (správa hesel, instalace aplikací, vnucení datového obsahu aj.)

2.2 ohrožení prostřednictvím IT prostředí MSM, ve kterém je MSM provozován - prostřednictvím systémových prostředků IT, u kterých (pokud nejsou řádně chráněny proti rizikům zneužití funkcionality ad bod A) tohoto dokumentu) hrozí riziko zneužití v MSM disponibilní funkcionality i získaných dat, setup i informací z provozu mobilů, a to prostřednictvím 3 osob – např. hackerů, kteří díky nekorektnímu IT prostředí, ve kterém je mobil s MSM provozován, budou schopni neoprávněně čerpat jak z funkcionality MSM tak v MSM od uživatelů shromážděných dat.

DÍLČÍ ZÁVĚR ZNALCE K BODU B/ ZADÁNÍ

V této chvíli (k lednu 2015) nelze k rizikům MSM uvést více, nicméně dle povahy produktu MSM z jeho veřejně deklarovaných vlastností lze dedukovat, že v jistých verzích MSM či formou návazných – neveřejných částí této aplikace – mohou být k dispozici i funkcionality typu odposlechu, a to jak mobilem vedených hovorů, tak na dálku provozovatelem MSM řízených prostorových odposlechů subjektů v dosahu daného mobilu, možného vedení zástupné komunikace (namísto vlastníka mobilu komunikuje 3 strana) aj.

Vlastní únik informací z MSM je de-facto prokázán již k dané době ve veřejnoprávních médiích publikovanými zprávami o jeho provozu v bezpečnostních strukturách ČR (např. zpráva zpravodajského serveru České noviny ze dne 18.12.2014 v 14:02 hod), otázka zda reálně došlo ke kompromitací dat z MSM ad bod 2.1 či 2.2 výše či jiným způsobem je však otázka primárně na orgány činné v trestním řízení.

3 **ad bod C) zadání - možné způsoby ověření reálného úniku informací o provozu mobilních zařízení, a kompromitace jejich dat - je provedena takto :**

Jak již uvedeno výše pod dílčím závěrem k bodu 2) zadání, byly v této věci po dohodě se zadavatelem kontaktovány spolupracující odborné subjekty (…. detaily anonymizovány) s tím, že pokud se daný subjekt pozitivně vyjádří k možnosti spolupráce na produktu Meraki MSM, pak bude možno realizovat následující ověření prokazatelného úniku informací takto :

3.1 prokázání instalace programové komponenty Meraki v zadavatelem, či ze strany orgánů činných v trestním řízení v této věci poskytnutém zařízení (mobil, tablet či PC/NB s OS Android, iOS Windows) a dále

3.2 vytěžení veškerých dostupných informací o provozu komponenty Meraki z takto poskytnutého zařízení ke zkoumání – obsah těchto informací však závisí na „stopách“ které po své činnosti zanechává v zařízení programová komponenta Meraki – další detaily anonymizovány.

Jelikož jak uvedeno pod dílčím závěrem k bodu 2) zadání, je únik informací z MSM de-facto prokázán, pak je s ohledem na výše uvedená rizika ke zvážení podání podnětu zadavatele k šetření orgánů činných v trestním řízení (dále OČTR) v této věci, pokud k uvedenému podání dojde pak do tohoto podání je potřeba formulovat následující :

3.3 získání rozhodnutí a podkladů (odborných i právně – legislativních) vedoucích k nákupu a nasazení produktů Meraki

3.4 získání řídících – organizačních normativů a odborných podkladů, definujících řízení nasazení a provozu produktů Meraki

3.5 zajištění přístupu OČTR a jejich specialistů do centrály provozu MSM, forenzní zajištění aktuální báze dat (i existujících záloh) vlastního MSM i tímto sledovaných zařízení pro zkoumání těchto dat ze strany OČTR a jejich specialistů

4 ZÁVĚR

Tímto lze zadáním požadovaná a v daném čase získaná, zde výše předložená fakta považovat k dané době za úplná .

Poznámka k anonymizované verzi z 2/2017

K informacím, předkládaným v tomto dokumentu, je nutno uvést, že tyto jsou poplatné dané době a stavu / situaci na trhu těchto produktů k závěru roku 2014 a stejně tak tehdejšímu stavu bezpečnosti komunikace v bezdrátových sítích i stavu zařízení na této síti komunikujících (od jejich operačního systému a aplikací až po tehdejší standardy i infrastrukturu bezdrát. sítí).

V současné situaci je nutno zejména respektovat fakt, že metody i produkty penetrace a naopak formy a praxe odhalování průniků, zabezpečení bezdrátových zařízení a jejich komunikace je jedno z nejdynamičtějších odvětví v branži IT, proto případná aplikace výše zmíněných faktů na současný stav by nutně musela projít aktualizací jak dle současné situace na trhu, tak dle konkretizace / aktualizace zadání směrem ke konkrétní události, či - byť hypoteticky- definované situaci.