MOBILNÍ ZAŘÍZENÍ ZAMĚSTNANCŮ JAKO HROZBA PRO POČÍTAČOVÉ SÍTĚ ORGANIZACÍ

THREATS TO COMPUTER NETWORKS ARISING FROM EMPLOYEES USING PERSONAL MOBILE DEVICES

Milan NOSKOVIČ
milan.noskovic@ioolb.izscr.cz

Abstract

This article discusses possible threats to computer networks arising from employees using personal mobile devices by that are not sufficiently secured. We look at the situation in small and medium-sized organizations with limited financial, technical and personnel resources.

We aim at a basic analysis of the most commonly used devices, their operating software and the resulting susceptibility to "infection."

The main types of security threats that are connected with the use of employees' own mobile devices within the corporate network are discussed.

We point to security options that are adequate in terms of financial, staffing and user friendliness. We cite examples of possible impacts of mobile devices viruses.

Key words

Mobile Device, Security Policy, Small and Medium Business Computer Network Security, Firewall, VPN - Virtual Private Network, Operating System, Android, iOS, Windows Mobile, IT Threat, Mobile Device Management - MDM, Enterprise Mobility Management – EMM.

ÚVOD

V organizacích se stále častěji povoluje zaměstnancům používat soukromá mobilní zařízení pro pracovní účely. Zejména kvůli použití firemního emailu, kalendáře a firemních aplikací. Tento trend se označuje jako BYOD (Bring Your Own Device), který na jednu stranu přináší větší úsporu zaměstnavatele, flexibilitu a vyšší efektivitu zaměstnanců, ale na druhou stranu přináší i větší bezpečnostní rizika, pokud nemají k dispozici bezpečný přístup k firemní síti, například zabezpečen pomocí VPN (virtual private network) klienta.

Společným jmenovatelem pro všechna „chytrá" mobilní zařízení je, že se vlastně jedná o malý počítač, který je neustále připojen k Internetu. Je na nich používán operační systém, součástí kterého je řada typů konektivit (mobilní síť, Wi-Fi, Wi-Fi Direct, Bluetooth, NFC, GPS atd.), internetový prohlížeč, emailový klient jak pro služební, tak pro soukromou poštu, možnost připojení ke kalendáři i k datům z firemního informačního systému, možnost instalovat aplikace atd. Většina uživatelů má na svých mobilních zařízeních nainstalovány nejen aplikace sloužící k pracovnímu využití, ale i aplikace sloužící pro zábavu.

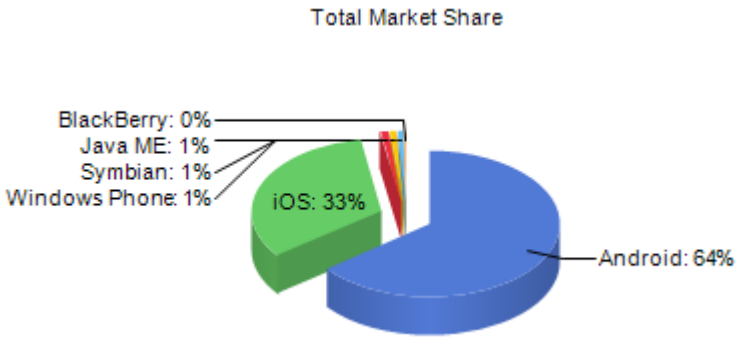
V našem případě jsme se konkrétně zabývali verzí OS Android 7.0 instalovaném na mobilním zařízení Samsung Galaxy S6 edge a na iOS verzi 10.3.3 instalovaném na mobilním zařízení Apple iPhone 6S.

1 Používané operační systémy na mobilních zařízeních

- Android – od Google
- iOS – operační systém mobilních zařízení Apple
- Windows Phone – od Microsoftu

Za zmínku ještě stojí starší nebo alternativní současné operační systémy, mezi které patří například:

- OS Jolla
- Symbian
- Blackberry OS
- Firefox OS (Alcatel)
- Tizen



Podíly různých operačních systémů na trhu – upraveno z NETMARKETSHARE [1]

Operating System	Total Market Share
Android	64.38%
iOS	33.09%
Windows Phone	0.89%
Symbian	0.70%
Java ME	0.64%
BlackBerry	0.28%
Samsung	0.01%
Bada	0.00%
Kindle	0.00%
HUAWEI	0.00%

Pro bezpečnost zařízení hraje důležitou roli, z jakých zdrojů mohou uživatelé instalovat aplikace.

- Android – oficiálním zdrojem je Google Play. Případné závadné aplikace mohou být firmou Google z tohoto úložiště odstraněny. Uživatelé ale mají možnost povolit i instalaci z libovolného jiného zdroje, a to buď jednorázově, nebo trvale. Tvůrci škodlivého

software pak postačuje např. umístit lákavý odkaz na stažení aplikace do reklamního banneru. Další riziko pak představuje možnost využití neoficiálního postupu pro navýšení uživatelských práv k operačnímu systému – „rooted“ zařízení.

- iOS – aplikace lze stahovat pouze z oficiálního zdroje App Store. Zde jsou firmou Apple aplikace předem kontrolovány na nezávadnost. Přesto i tak může dojít k dočasnému vystavení problematického programu. Podobně jako v případě Androidu, existuje i zde neoficiální postup pro navýšení práv – „jailbroken“ zařízení pak umožňuje instalaci z libovolných zdrojů.
- Windows Phone – aplikace lze nainstalovat z oficiálního Microsoft Store, ale systém umožňuje i celou řadu dalších možností instalace.

2 Průzkumy a statistické údaje

Se statistikou přišla společnost Skycure, specializující se právě na bezpečnost mobilních zařízení. Obecně lze říci, že množství útoků na mobilní zařízení roste a podstatný díl na tom mají i samotní uživatelé, kteří dostatečně nedbají na jejich bezpečnost. Podle Skycure není v 71 % zařízení s Androidem nainstalován aktuální bezpečnostní patch. A právě tato zařízení jsou nejčastěji mezi napadenými. Průzkum tak potvrzuje nedávno zveřejněnou zprávu Googlu, podle které na zhruba polovině zařízení s Androidem neproběhla aktualizace s potřebným bezpečnostním patchem už přinejmenším rok. Mnozí uživatelé argumentují, že systémové aktualizace snižují výkon jejich zařízení, a proto se jim vyhýbají. Odborníci však kontrují tím, že takové uvažování je nesmyslné, jelikož škodlivý software, kterému takovým konáním uvolňujeme cestu, ve finále výkon snižuje mnohem víc. [2]

3 Možná rizika použití donesených zařízení pro firemní síť

Používání mobilních zařízení pro přístup k firemní síti přináší pro uživatele vyšší produktivitu a možnost být stále „on-line“. Na druhou stranu však vzniká celá řada rizik, která jsou ve srovnání se zařízeními ve firemní správě obtížněji zvladatelná [3]. Pokud není těmto rizikům věnována dostatečná pozornost, může dojít k významným škodám i přesto, že zabezpečení pevné sítě byla věnována dostatečná pozornost a vynaloženy značné investice.

Mezi hlavní typy rizik patří:

a) Únik citlivých firemních informací

V současné době se činnost závadných programů pro mobilní zařízení zaměřuje hlavně na získání citlivých informací, například přístupových informací elektronického bankovnictví, čísel platebních karet, zadávaných hesel. Prevence těchto rizik nabývá na významu v souvislosti s nastávající platností Obecného nařízení o ochraně osobních údajů (GDPR). Mezi hlavní způsoby patří:

- Instalace škodlivého programu (malware), který je zaměřen na skryté získávání cenných údajů. Uživatel zařízení si takový program, který obvykle slibuje zdarma některé atraktivní funkce, většinou stáhne z webu mimo oficiální zdroje. Získaná data jsou pak odesílána na server tvůrců malware a mohou být následně zneužita.
- Ztráta, odcizení nebo prodej mobilního zařízení. Zařízení používané delší dobu ve firemní síti v sobě může obsahovat mnoho důležitých dat. Typicky se jedná o zprávy elektronické pošty, uložené firemní soubory, přístupové údaje nebo nakonfigurované VPN připojení. Pokud není zařízení dostatečně chráněno přístupovým kódem a šifrováním, může dojít při

jeho ztrátě nebo odcizení k úniku velmi důležitých informací nebo k získání neautorizovaného přístupu do firemní sítě. Stejná situace může nastat i při prodeji mobilního zařízení, pokud majitel opomene předem zajistit výmaz dat.

- Připojení k cizí nezabezpečené nebo podvržené WiFi síti umožňuje provozovateli takové sítě sledovat obsah přenášených dat. V některých případech může být využito i falešných certifikátů pro útoky typu „man-in-the-middle“ a získat tak přístup i k zabezpečené komunikaci.

b) Napadení ostatních zařízení ve firemní síti

Napadené mobilní zařízení by mohlo pro šíření nákazy na standardní počítače ve firemní síti využít například tyto způsoby:

- Závadná aplikace nainstalovaná na telefonu může v souborovém systému přístroje umístit spustitelný soubor s virem pro Windows a přidat soubor autorun.inf. Pokud po připojení mobilu k počítači USB kabelem vidí PC toto zařízení jako externí disk, může dojít k automatickému spuštění viru a následnému zavlečení nákazy do PC. Záleží však na tom, v jakém režimu se mobilní zařízení prezentují přes USB hostitelskému počítači. Uvedené riziko se týká pouze režimu USB Mass Storage. [4]
- Přímé napadení počítačů v lokální síti přes WiFi připojení z kompromitovaného mobilního zařízení, například s využitím některé známé zranitelnosti v OS Windows, nyní nepředstavuje významné riziko.
- Hypotetickou možností je existence škodlivého programu, který by pozměnil funkci telefonu tak, aby se po připojení k PC prezentoval jako USB klávesnice a myš. Pak by mohl vyslat do počítače libovolné příkazy, které by například mohly z internetu stáhnout a spustit jiný malware dříve, než si uživatel všimne nečekaných akcí. Činnost takového viru ale vyžaduje modifikaci ovladačů jádra telefonu, a proto se zřejmě podobný malware v praxi nevyskytuje – i když program, který udělá z telefonu klávesnici a myš, skutečně existuje [5].

c) Ostatní rizika

- Některé typy malware mohou zneužít mobilní zařízení pro rozesílání spamu. Pokud je přitom toto zařízení připojeno do firemní sítě, je kompromitována veřejná IP adresa organizace a může dojít k jejímu zařazení do databáze rozesilatelů spamu. Následně je tím pak narušen provoz firemních poštovních serverů.
- Napadení telefonu některým typem ransomware nemusí představovat přímý dopad na dostupnost firemních dat, protože jejich originály jsou uloženy na podnikových serverech nebo osobních počítačích. Součástí napadení ale může být i jiný malware, který se bude snažit např. o přístup k citlivým údajům.

4 Způsoby ochrany proti rizikům

Vzhledem k rozsáhlosti rizik, která představují použití vlastních mobilních zařízení pro firemní síť, je nutné volit taková komplexní bezpečnostní opatření, která pokrývají všechny oblasti nasazení, používání a monitorování mobilních zařízení. Zvolené řešení by mělo také být v souladu s doporučením příslušných norem ISO/IEC 27002, EU 2016/679 (GDPR).

Prvním krokem je stanovení firemní politiky, která bude definovat zásady pro používání vlastních mobilních zařízení zaměstnanců ve firemní síti. Její součástí by mělo být určení rozsahu použití, stanovení kompetencí a odpovědnosti zaměstnanců.

Důležité je také vytvoření závazných bezpečnostních pokynů pro uživatele mobilních zařízení, kteří pak budou s tímto dokumentem seznámeni a náležitě vyškoleni. Mezi hlavní požadavky může patřit:

- Ochrana přístupu do zařízení biometrickými údaji nebo heslem. V případě hesla je potřeba vyžadovat buď dostatečnou délku, nebo povolit automatické vymazání telefonu po několika neúspěšných zadáních.
- Povolit šifrování dat (u iOS zapnuto implicitně, u Androidu nutno povolit).
- Instalace aplikací jen z oficiálních zdrojů, zákaz zásahů do operačního systému (rooting, jailbreaking).
- Nutnost okamžitě nahlásit případnou ztrátu nebo odcizení zařízení kompetentním osobám ve firmě, aby mohlo dojít k adekvátním opatřením (změna hesla, zneplatnění certifikátu, vzdálený výmaz). A také povinnost zaměstnanců zajistit výmaz telefonu před jeho prodejem nebo předáním do opravy.

Součástí poučení by měl být i souhlas uživatele s instalací příslušného bezpečnostního software.

Před použitím telefonu ve firemní síti je potřebné na něj nainstalovat některý kvalitní antivirový program. Ten by měl optimálně nejen zabránit instalaci závadných aplikací a odstranit již nainstalovaný malware, ale i sledovat podezřelé chování aplikací, detekovat útoky na SSL komunikaci, rozpoznat „nepřátelské“ sítě a provést potřebné ochranné kroky i bez zásahu uživatele. Software by také měl být schopen blokovat rooted/jailbroken zařízení, rozpoznat zranitelnosti OS a vyzvat uživatele k jeho upgrade.

Pro připojení mobilních zařízení uvnitř firemní sítě by měl být určen samostatný segment WiFi sítě oddělený od ostatních částí pomocí firewallu. Na něm by měl být povolen pouze provoz nezbytný pro používané aplikace. Tím se omezí jak možnost případného šíření škodlivého kódu, tak i přístup k interním zdrojům, které mobilní aplikace nevyužívají.

Aby při připojení mobilních zařízení k veřejným nezabezpečeným WiFi sítím nemohlo dojít k únikům dat zachycením komunikace vyměňované přes Internet s firemní sítí, je vhodné skrýt provoz do VPN připojení. Toto VPN spojení může sloužit buď pro veškerou komunikaci zařízení, nebo jen pro data přenášená firemními aplikacemi. První varianta umožní zabezpečit firemním firewallem i komunikaci zařízení do Internetu, představuje však vyšší zátěž pro telefony i firemní síť.

5 Systémy pro správu mobilních zařízení

Protože vlastní mobilní zařízení uživatelů nejsou v přímé správě IT oddělení, je vhodné implementovat takový centrální způsob řízení jejich přístupu do firemní sítě, který zajistí, že mobilní zařízení budou splňovat všechny stanovené bezpečnostní požadavky a umožní jejich vzdálenou správu a monitorování. Tyto systémy jsou označovány jako Mobile device management – MDM. Mezi jejich hlavní funkce patří:

- Vynucení přístupových politik, jako je přítomnost antivirového programu, ochrana dostatečně silným heslem nebo biometrií, odmítnutí jailbroken/rooted zařízení, šifrování dat uložených na mobilním zařízení, oddělení firemních a soukromých dat, vytvoření VPN
- Registrace nových zařízení, vazba uživatelů na firemní databázi, například Microsoft AD
- Možnost vzdálené lokalizace telefonu a jeho kompletní nebo částečné vymazání v případě ztráty nebo odcizení
- Monitorování provozu

Systémy MDM mohou být součástí komplexnějších systémů pro správu, které zahrnují i další aspekty provozu mobilních zařízení, jako je správa aplikací, dat a poštovních klientů. Tato řešení jsou označována EMM – Enterprise mobility management.

Mezi představitele řešení pro správu mobilních zařízení patří mimo jiné VMware AirWatch, Citrix XenMobile, IBM MaaS360 nebo Microsoft Itune [6].

Například platforma AirWatch zahrnuje řešení pro správu mobilních zařízení, správu mobilních aplikací i řadu dalších funkcionalit – oddělení soukromých a firemních dat na jednom mobilním zařízení, bezpečnou distribuci obsahu na tato zařízení na základě řady pravidel, včetně například regionu, v němž se zařízení nachází, synchronizaci obsahu, bezpečný přístup k webu, kontejnerizaci aplikací pro zajištění vyšší bezpečnosti nebo snadnější správy a nově třeba i řešení pro tvorbu a sdílení firemních videí.

ZÁVĚR

Použití vlastních zařízení zaměstnanců (BYOD) přináší nejen vyšší produktivitu, úsporu firemních nákladů, možnost být stále on-line, ale také řadu bezpečnostních rizik. Mezi ně patří hlavně možnost úniku citlivých firemních dat buď činností malware, nebo při ztrátě a odcizení zařízení. Rizikem je také připojování zařízení do veřejných sítí, kde může docházet k zachycování komunikace. Vyloučit nelze ani zneužití mobilního zařízení pro přímé napadení firemní sítě.

Proto je nutné stanovit funkční firemní bezpečností politiku, která bude určovat všechny zásady, které je nutné při přístupu mobilních zařízení splnit. Bude zahrnovat jak požadavky na konfiguraci mobilních zařízení a přístupové infrastruktury, tak i kompetence zodpovědnosti jednotlivých pracovníků. Mezi hlavní technická opatření patří zabezpečení přístupu silným heslem, blokování modifikovaných (rooted/jailbroken) zařízení, použití antivirového programu, šifrování, možnost vzdálené lokalizace a výmazu zařízení, ochrana komunikace pomocí VPN a oddělení přístupu ve firemní síti firewallem.

Aby bylo možné zajistit, že připojovaná zařízení stanovené podmínky splňují, je vhodné nasazení některého z přístupových systémů typu MDM (Mobile device management), případně komplexnějšího EMM (Enterprise mobility management). Ty zajistí centrální vynucení bezpečnostních profilů, monitoring, vzdálené vymazání zařízení, případně další funkce, jako je správa mobilních aplikací, obsahu a pošty.

Příspěvek vznikl v rámci projektu VI20152020009.

Literatura

[1] NETMARKETSHARE. *Operating system market share* [online]. [cit. 2017-07-4]. Dostupné z: https://www.netmarketshare.com/operating-system-market-share.aspx?qprid=8&qpcustomd=1

[2] COMPUTERWORLD. *Zařízení s Androidem jsou nebezpečná, varuje průzkum* [online]. [cit. 2017-04-27]. Dostupné z: http://computerworld.cz/securityworld/zarizeni-s-androidem-jsou-nebezpecne-varuje-pruzkum-53762

[3] Symantec *Mobile Threat Protection: A Holistic Approach to Securing Mobile Data and Devices* [online]. [cit. 2017-09-11]. Dostupné z: https://www.symantec.com/content/dam/symantec/docs/white-papers/sans-mobile-threat-protection-a-holistic-approach.pdf

[4] How-to Geek. *Android USB Connections Explained: MTP, PTP, and USB Mass Storage* [online]. [cit. 2017-09-11]. Dostupné z: https://www.howtogeek.com/192732/ android-usb-connections-explained-mtp-ptp-and-usb-mass-storage/
[5] Google Play. *USB keyboard* [online]. [cit. 2017-09-11]. Dostupné z: https://play.google.com/store/apps/details?id=remote.hid.keyboard.client&hl=cs
[6] PCMAG. *The Best Mobile Device Management (MDM) Solutions of 2017* [online]. [cit. 2017-09-11]. Dostupné z https://www.pcmag.com/article/342695/the-best-mobile-device-management-mdm-software