

Mobilná bezpečnost

*e*FOCUS



Mobilita motor súčasného IT

9,5 Mld.

Užívateľov mobilných zariadení do roku 2020.

90%

Užívateľov mobilných služieb bude do roku 2020 používať mobilný BB.

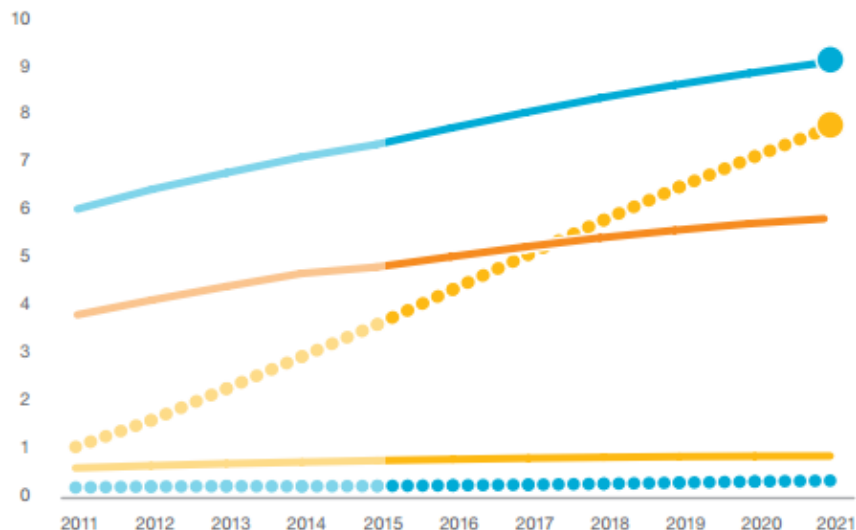
6,1 Mld.

Užívateľov smartphonov očakávame do roku 2020.

90%

Svetovej populácie nad 6 rokov bude mať do roku 2020 mobilný telefón.

Subscriptions/lines, subscribers (billion)



- Mobile subscriptions
- Mobile broadband subscriptions
- Mobile subscribers
- Fixed broadband subscriptions
- Mobile PCs, tablets and mobile router subscriptions

Unikátne výzvy mobilného IT

Špecifikom mobilného IT je fakt, že zamestnanci pristupujú k senzitívnym firemným dátam z privátnych aj verejných sietí a veľkého množstva súkromných aj firemných mobilných zariadení.

Mobilné zariadenia pracujúce **mimo perimeter firemnej siete** vytvárajú riziko útoku z verejných sietí.

Veľké množstvo druhov mobilných zariadení a mobilných OS.

Užívatelia požadujú **prístup k firemným údajom** cez ich mobilné zariadenia čím zvyšujú riziko úniku dát.



Zabezpečenie mobilných telefónov **zaťažuje batériu** mobilného zariadenia.

Mobilné zariadenia vytvárajú riziko krádeže dát z **mobilného zariadenia aj z mobilnej siete.**

Nemožnosť **admin prístupu a dohľadu nad sieťou** sťažuje kontrolu a detekciu prípadných hrozieb.

Riziká mobilného IT

Riziká mobilného IT

263 % nárast mobilného malware za posledných 12 mesiacov.

82 % spoločností priznalo bezpečnostný incident spojený s mobilnými zariadeniami.

80 % zamestnancov používa súkromné mobilné zariadenie na prístup k firemným dátam.

75 % oincidentov spojených s mobilnými zariadeniami je zapríčinených nesprávnou konfiguráciou.

TOP 5 rizikové faktory podľa CIO

- 1 **Strata dát z dôvody straty, krádeže mobilného zariadenia** (vyše 70%)
- 2 **Mobilný malware** (70%)
- 3 **Nedostatočná ochrana dát na mobilných zariadeniach** (65%)
- 4 **Možné zákonné požiadavky spojené s vynucovaním bezpečnostných politík na BYOD zariadeniach** (vyše 65%)
- 5 **Presadzovanie akceptovateľných bezpečnostných politík na mobilných zariadeniach** (Vyše 60%)

Aktuálne druhy mobilných hrozieb

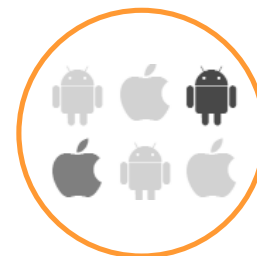


MALWARE:

Dobre známy výraz spopularizovaný mediálne známymi kauzami straty dát, ukradnutými číslami kreditných kariet, krádežami fotografií a iným... Malware sa stalo všadeprítomným fenoménom rozšíreným pomocou obchodov s aplikáciami, najmä tretích strán.

REPACKAGED APPS, APP EXPLOITS:

Jedným zo spôsobov útočníkov ako sa dostať do mobilných zariadení je prebalenie populárnych aplikácií s pridaním škodlivého kódu a ich uverejnenie zadarmo v aplikačných obchodoch tretích strán.



OS A APLIKAČNÉ EXPLOITY:

Mobilné zraniteľnosti, exploits - chyby umožňujúce útočníkom úplné prevzatie správy zariadenia a získanie kompletných dát zo zariadenia.

SNIFFING, MITM (MAN-IN-THE-MIDDLE):

Odchyťovanie sieťovej prevádzky, alebo jej presmerovanie pomocou zneužitia funkcií automatického pripájania k súkromným, alebo verejným WiFi sieťam. Útočníci môžu odchytiť aj prevádzku zariadení s deaktivovaným WiFi pomocou falošných BTS staníc.



Príklady známych hrozieb



Stagefright ohrozuje 90% Android zariadení

Využíva zraniteľnosť nájdenú v Android mediálnej knižnici. Keď pomocou infikovanej MMS útočník získava kontrolu nad zariadením pomocou zneužitia funkcie "multimedia preview".



XcodeGhost Attacks

Ovplyvňuje všetky iOS zariadenia inštalovaním infikovanej aplikácie. Infikované aplikácie sa môžu nachádzať aj v oficiálnom Apple App Store. Do dnešných dní bolo identifikovaných a odstránených viac ako 4000 aplikácií.



Keyraider, ukradol viac ako 225,000 Apple účtov

Malware ovplyvňujúce Jaibroken zariadenia kradnúci mená, heslá, certifikáty a dokonca aj privátne šifrovacie kľúče. Pomocou týchto dát sa útočník rýchlo môže dostať k firemnej pošte, dokumentom, atď...



YiSpecter Stjane kradnúci dáta z iOS zariadení

Pomocou sociálneho inžinierstva sa šíriaci malware útočiaci aj na nejailbroken zariadenia inštaláciou infikovaného profilu. Môže meniť, inštalovať a spustiť aplikácie bez súhlasu užívateľa.

Ako zabezpečiť mobilné zariadenia?

Vyriešiť HLAVNÉ RIZIKOVÉ FAKTORY MOBILNÉHO IT:

- BYOD zariadenia a politiky
- Stratu dát
- Malware

Ochrániť VŠETKY VRSTVY :

- Prístup ku mobilnému zariadeniu
- Aplikácie a OS zariadenia
- Sieť pripájajúcu zariadenie

POKRYŤ 3 PILIERE MOBILNEJ EZPEČNOSTI:

Bezpečnosť zariadenia

- Bezpečnosť mobilného zariadenia
- Antimalware
- Statická analýza kódu

Reputácia

- Reputácia aplikácií
- Reputácia zariadení
- Mobilné DLP

MDM and tradičné zabezpečenie Mobilných zariadení

- Mobile device manažment
- Kontajnerizácia dát
- Wrappovanie aplikácií

Návrh riešenia

AGREGÁCIA Bezpečnostných Technológií

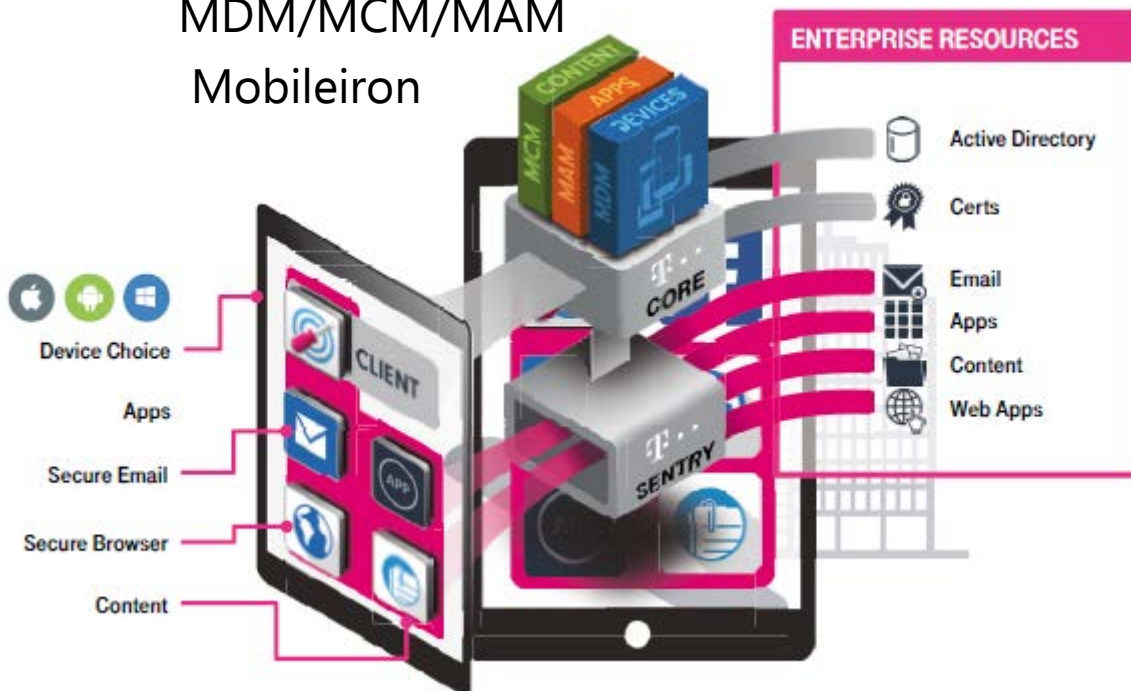
- Mobile Device Management
- Kontajnerizácia
- Hardening aplikácií
- Zabezpečenie zariadenia



Mobile Endpoint Security
Zimperium

MDM/MCM/MAM

Mobileiron



Ďakujeme za pozornost



Zimperium MTP demo MITM attack

- Unprotected device
- Protected device

<https://www.youtube.com/watch?v=AGCm5WWIB4k>