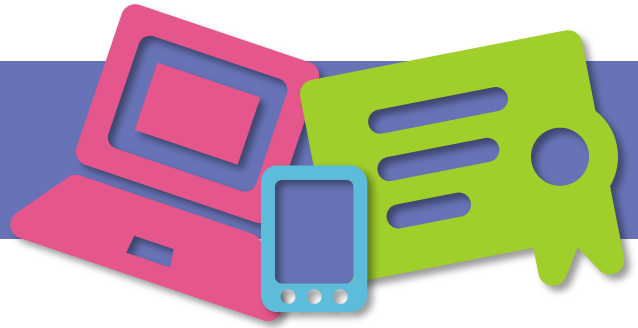
SECURITY 2014

22. ročník konference o bezpečnosti v ICT



BYOD – nebezpečí, které musíme akceptovat

Richard Voigts

DCD Publishing/Reseller Magazine

BYOD

- BYOD + BYOx
  - Bring Your Own Device (mobilní zařízení)
- BYOD, BYOS, BYOA, BYOx

- Gartner, IDC: cca 2,5 miliardy mobilních zařízení ročně, v roce 2013 více smartphonů než tlf.
- Cisco: do roku 2020 – 50 miliard připojených zařízení (vč. internetu věcí)

BYOD – neznámý vesmír

- Fyzický prostor – známe, při přechodu ulice se umíme rozhlédnout.

- Kyberprostor – neznáme, jako pro Evropana rozdíl mezi alkoholem a novodobou či cizokrajnou drogou. Na tuto kocovinu neexistuje guru.

BYOD – bezpečnost

- Krádeže dat – 23 mld. USD ročně, krádeže ID, debetní karta – 1 USD, PIN – 10 USD, zdravotní karta 50 USD (Safetica)
- FBI: cybercrime je hodnotnější než obchod s drogami.
  - Kolik stojí vaše data? Kolik stojí váš ukradený notebook? (Intel -> 100 000 Kč)
  - Máte bezpečnostní politiku pro ztrátu firemního smartphonu?
  - Kolikrát už jste dohledali nebo „zabili“ smartphone na dálku?
- Eugene Kaspersky: „Vše už bylo alespoň jednou ukradeno, vše má svého kupce.“

BYOD – rizika x přínosy

- **Rizika a problémy**:
  - Bezpečnostní – „pouhé“ rozšíření rizik.
  - Technická – jak zařízení zapojit (doména, VPN)
  - Právní – BYOD (vlastní zařízení) navozuje neřešitelnou právní situaci.
  - Narůstají s přechodem do cloudu.

- **Přínosy (a problémy)**:
  - Ekonomické – povolit vlastní (=ušetřit) x zaplatit podnikové zařízení (=náklady)?
  - Produktivita – neoddiskutovatelný nárůst!

BYOD – aspekty

- Technické – jak „to“ připojit
- Bezpečnostní – jak „to“ (podnik i uživatele ochránit)
- Ekonomické – kolik „to“ bude stát, co to přinese
- Právní – jak s „tím“ naložit v případě selhání

BYOD a ČR

- Intel: Firmy ve střední Evropě s přijímáním trendu příliš nespěchají. (762 dotazovaných firem)
- Průměr ve střední Evropě – 12 %, ČR – 14 %, SK – 9,8 %, HU – 18 %, PL – 7,5 %
- Gartner, IDC: cca 2,5 miliardy prodaných mobilních zařízení ročně.
- Zajímá vás statistika, nebo bezpečnost vašeho podniku? Kolik lidí u vás nemá smartphone? Kolik z těch, co jej má, nemůže do e-mailu a sítě vaší organizace?

BYOD – jak se k vetřelci postavit?

- BYOD – ignorovat, zakázat, akceptovat, podporovat?
  - Ignorovat? Neřešit?
    - Nelze...
  - Zakázat? (sklad TD; citlivé provozy – Nokia GSM bez fotoaparátu)?
    - Lze, ale s vysokými náklady a se ztrátou produktivity.
  - Akceptovat BYOD? => Ochránit organizaci!
  - Podporovat BYOD? => Ochránit organizaci!

BYOD – akceptovat a ochránit

- Jiří Devát, Cisco Systems:
  - BYOD není nebezpečím, ale principem, podle kterého je bezpečnost řešena!
    - „V okamžiku **akceptování** distribuované bezpečnosti povoleného prostoru, už není **BYOD** nebezpečím, ale **principem**, podle kterého je bezpečnost řešena. Existuje snaha vědět, kdo, z jakého zařízení a s jakými právy se připojuje právě k síti, podle toho rozlišovat přístupová hesla, řídit provoz v síti a směřovat komunikaci těmi kanály, které jsou **přiměřeně bezpečné** pro daný účel.“ (pro Reseller Magazine, 2014)

BYOD – připojení a nebezpečí

- KPMG: osobní mobilní zařízení – osobní komunikace, zábava, osobní finance, pracovní e-maily => kritická podniková data
  - Wi-Fi + GSM – internet + odesílání podvodných SMS na drahá čísla (Android).
    - (Ono stačí nevypnout/nezablokovat datové služby při cestě do ciziny.)
  - Internet – procento napadení vzrůstá s exponenciálním počtem připojených zařízení.
  - Bluetooth – spuštění na dálku (i při vypnutém přístroji!!!), aktivace kamery ve smartphonu...

- Kolik máte ve vaší organizaci připojených mobilních zařízení vy?

BYOD – zařízení a OS

- Pouze smartphone, tabletPC/mediatablet?
  - Android, iOS, Windows Mobile, Symbian
  - Ostatní: Windows 7/8.1, MacOS – spíše firemní zařízení
- Ale ne… také zařízení bez OS!
  - Fotoaparát nejen s Wi-Fi, ale i mikrofonem?
  - Další zařízení v kyberprostoru internetu 50 miliard věcí...? (Dnes ještě „pouhých“ 15 miliard věcí.)
  - Flash paměti (Stuxnet)

BYOD – nebezpečí z internetu

- Android = dobře popsaný systém => dobře napadnutelný.
- Windows Mobile – nebezpečí bude narůstat s pronikáním do podnikové sféry.
- MacOS, iOS – zpravidla nutná interakce člověka.
- Zařízení s MacOS a iOS spíše nositelem podnikové nákazy.
- Ale...
  - AV Comparatives: mýtus o bezpečných OS? Malware a botnety už i na MacOS!

BYOD – lidé + povědomí

- Problém „mezi klávesnicí a židlí“ > 90 % případů (úmysl, nedbalost, nevědomí)
  - Rozdíl mezi MS Windows a MS Office? Nezná jej 8 až 9 lidí z 10!
    - Natož pak phishing, botnet, farming...
  - Není povědomí o služebním tajemství – úniky informací (lidský faktor + neošetření procesů).
  - Sociální inženýrství („Vezeme naléhavý případ!“; Dejte mi Petra! (no přece Kellnera), jeho mobil, přístup do systému. (Neošetření procesů.)

- Lidé : 95 % - > 90 % od roku 1998 do roku 2013

BYOD – ochrana

- 1. Lidé
  - omezit rizika lidského faktoru
  - restrikce
  - osvěta
- 2. Procesy – zmapovat, nasadit
- 3. Technologie
  - celostní ochrana, monitoring provozu v sítích
  - ochránit osamocené zařízení, které se může připojit kamkoliv (v cloudu)

- Fortinet: Y-Generation – přes 50 % lidí mezi 20 – 30 lety připouští vědomé porušení pravidel!

BYOD – lidé a procesy

- Audit – osvěta, školení – měření – kontrola – audit – opakování...
- Vždycky jsme to tak přece dělali, nám se nemůže nic stát...
- My jsme tak malá firma, co by u nás hledali...
  - Pouze do té doby, než se zjistí, že dodává do Škody Auto – třeba čisticí prostředky. Může následovat objednávka v pdf s hypertextovým odkazem...

BYOD – technologie

- Restrikce – pouze částečný přístup a pouze schváleným zařízením (MAC)
- Vynucení politik vůči uživatelům, zablokované USB porty apod.
- Oddělený přístup hostů k internetu ve firmě

- Celostní přístup, nikoliv pouhá ochrana koncových zařízení!
  - Restrikce pro koncová zařízení, sledování neobvyklého chování v síti, ochrana okrajů (perimetru) sítí.

BYOD – bezpečnostní díry

- Hesla
  - Jednoduchá až hloupá
    - 1. jméno pet (psa, kočky)
    - 2. syna
    - 3. dcery...
    - X. nejlidnatějšího města...)
  - Připíchnutá na nástěnce kvůli vynucování častých změn
  - Bez hesla – nastavený trvalý přístup k webové stránce/bance
  - 000000 – heslo k odpálení US jaderných raket
  - Richard Feynman, jaderný fyzik: Na zakázku US armády odemykal její trezory defaultním továrním heslem. Nikdo je totiž nezměnil...
- Kolik vašich zaměstnanců vůbec používá PIN do smartphonu?
- Kritické provozy – jiné způsoby autentizace

BYOD – díry v praxi

- Příklady děr v procesech
  - KB – Login ID, Password, ale i Remember ID v aplikaci pro iOS
  - Microsoft SkyDrive/OneDrive/OneNote – vynucení silného hesla x možnost trvalého přihlášení. (Master OneNote samozřejmě součástí Office na HDD uživatele.)
- Jak je na tom váš systém, intranet, web, VPN?
  - Lze se do nich trvale také přihlásit?

BYOD + IT odborníci

- J. V. Binder, Apogeo Esteem:
  - Dříve – hádky o Unix a Novell x Windows XY a bezpečnostní stupně – B2, certifikace NATO atd.
  - Dnes – přístup správců do kritických systémů hračkou s Androidem bez jakékoliv certifikace.

- Cisco:
  - V současné době chybí celosvětově více než 1 milion guru – (paranoidních) odborníků na bezpečnost!

BYOD – kvíz

- Kdo zde (ne)máte smartphone?
- Kdo máte tablet PC?
- Používáte jej ke služebním účelům?
- Vypínáte Bluetooth?
- Vypínáte smartphone na noc?
- Vyndáváte ze něj akumulátor?
- Zablokoval váš správce některé jeho funkce?
- Máte nainstalovaného bezpečnostního klienta?
- Pokud ne, zamkli jste doma dveře?

BYOD – možná východiska

- J. V. Binder, Apogeo – jak a na co se při příchodu BYOD orientovat:
  - Opřít se o zákony, podnikové směrnice, další dokumenty.
  - Nejprve raději změny pracovních smluv místo MDM.(Mobile Device Management – Gartner: 20 % programů BYOD selže, MDM je příliš restriktivní)
  - Postupovat stejně jako u soukromého vozidla pro služební účely.

- Vladimír Rohel (NBÚ), Aleš Špidla (MIB+MPSV): Nutnost přijetí zákona, šíření osvěty v každé organizaci!

BYOD – zákon a budoucnost

- Zákon o kybernetické bezpečnosti + prováděcí vyhláška v roce 2015
- Lepší vymahatelnost práva
- Bude-li napadena třetí strana, budete muset umět vysvětlit, že...
- Budete se o bezpečnost svého systému **muset** starat!
- BYOD: komu a jak povolit...
  - Abyste mohli vysvětlit, že: Kdo, kdy, co, komu, ev. s kým...

SECURITY 2014

22. ročník konference o bezpečnosti v ICT

Děkuji za pozornost.

Richard Voigts

DCD Publishing

voigts@dcd.cz; 606 761 826