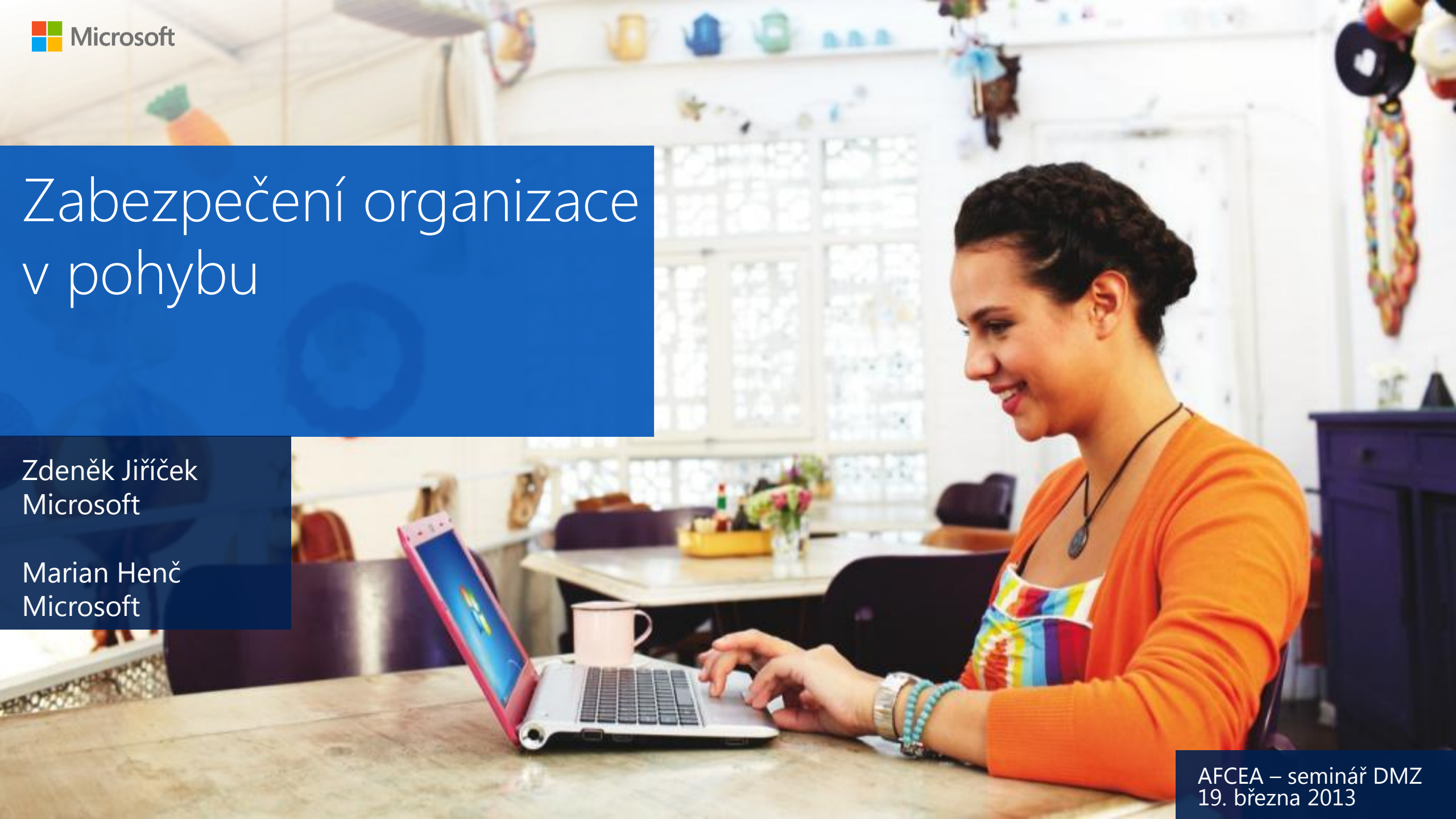
Microsoft

Zabezpečení organizace v pohybu

Zdeněk Jiříček
Microsoft

Marian Henč
Microsoft



AFCEA – seminář DMZ
19. března 2013

Útoky na DMZ od ekonomické krize

Je to živnost

- Dříve pro svoje ego, nyní pro peníze
- Trh bez hranic, noví hráči
- Cílený hacking na objednávku

Firemní mobilita

- Nové pojetí DMZ
- BYOD: vynutitelnost politik?
- Útoky na klientské stanice
- Vzdálený přístup

Sociální engineering

- Phishing -> škodlivý website
- Falešný antivirus
- Download kodeků k filmům
- „Dárky“ – USB zařízení

Pokročilé metody

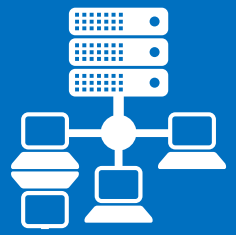
- Informace ze sociálních sítí
- Metasploit framework
- Blackhole exploit kit
- Trojany -> Botnety
- Rootkity obcházející Antiviry

Realita malwaru na klientských stanicích

www.microsoft.com/security/MMPC

Scénáře správy zařízení

Správa v doménovém prostředí

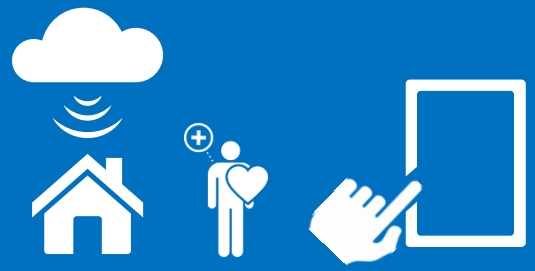


- ✓ Maximálně zabezpečené zařízení
- ✓ Možnost vynucení bezpečnostních politik
- ✓ Šifrování a vícefaktorová autentizace
- ✓ Výhody vycházející z vlastností Windows 7/8 (Bitlocker, Secure Boot, Dynamic Access…)

Správa nativním protokolem mobilních zařízení

- ✓ Omezené možnosti zabezpečení
- ✓ Nesourodá řešení třetích stran pro zabezpečení
- ✓ Vynutitelnost granularity politik je nízká

Řešení postavená na konzumerizaci IT



- ✓ Zařízení spravované samotným uživatelem
- ✓ Komunikace pomocí veřejných „free“ emailových služeb (Gmail, Hotmail)
- ✓ Správce sítě nemá žádný dohled nad zařízením

Správa v doménovém prostředí

- Maximální správa pomocí Group Policy v Active Directory
- Bezpečnostní funkce a vlastnosti Windows 8
  (Bitlocker, Bitlocker To Go, Trusted, Measured Boot, UEFI,
  Virtual Smart Card, Trusted Platform Module-TPM)
- Centrální server pro správu
  (System Center - ConfigMgr, OpsMgr, Endpoint Protection atd.)
- Reverzní proxy server (Unified Access Gateway)
- Externí přístup do korporátní sítě bez VPN (Direct Access)

Správa nativním protokolem mobilních zařízení

- Správa pomocí Exchange ActiveSync (EAS)
  - Původně určen pro synchronizaci emailů mezi Exchange serverem a mobilním telefonem
  - Bezpečnostní funkce:
    - Remote Wipe (vzdálené vymazání zařízení)
    - Device Password Policies (min. délka PIN, alfanumerické znaky, historie hesel atd.)
    - Device Encryption Policies (šifrování mobilního zařízení)
- Správa pomocí centrálního nástroje (ConfigMgr + Intune)
  - Správa mobilních zařízení přes všechny platformy (Windows RT, Windows Phone, iOS, Android)

Správa klientů s využitím cloudu

Řešení postavená na konzumerizaci IT

- Uživatel si přinese své vlastní zařízení do organizace (BYOD)
- Zabezpečení zařízení je na samotném uživateli
  - Velká pravděpodobnost úniku dat
- Obtížné připojení do organizační sítě
- Řešení problému
  - Začlenit zařízení do domény (zařízení s Windows)
  - Pokud toto není možné
    - Virtual Desktop Infrastructure (VDI z Windows, OS X, Linux atd.)
    - Vynutit bezpečnostní politiky (EAS, ConfigMgr, Intune – lze na Windows RT, Windows Phone, iOS, Android)
    - Windows To Go (Windows 8 na jakémkoliv PC z USB)

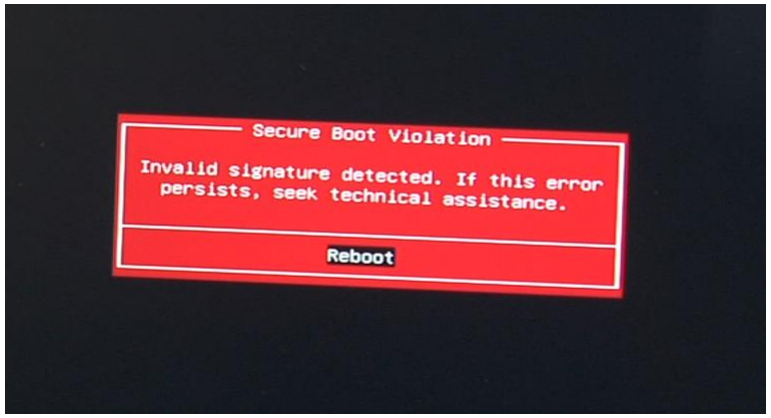
Bezpečnostní funkce Windows 8

Windows

UEFI - Unified Extensible Firmware Interface

- Standardní vylepšení BIOSu na nových PC
- Certifikáty uloženy v UEFI při výrobě počítače
- Certifikáty jak pro firmware jednotlivých hardwarových komponent s vlastními ROM BIOSy, tak certifikáty pro boot loadery
- Certifikát boot loaderu musí pasovat na certifikát v UEFI (UEFI v sobě mají tabulku povolených, případně i nepovolených certifikátů)

- UEFI will only launch a verified OS loader – such as in Windows 8
- Malware cannot switch the boot loader



Trusted Boot: Early Load Anti-Malware

Windows 7

Malware nabootuje před Windows a antimalwarem

- Malware se ukryje a zůstane nedetekován
- Systém může být kompromitován ještě před startem antimalwarového softwaru

Windows 8

Trusted Boot spustí antimalware v bootovacím procesu dříve

- Ovladač Early Load Anti-Malware (ELAM) je speciálně podepsán Microsoftem
- Windows nastartují antimalware před bootovacími ovladači třetích stran
- Malware takto nemůže obejít inspekci antimalwarového softwaru

Šifrování disku, části disku a USB flash disků

BitLocker

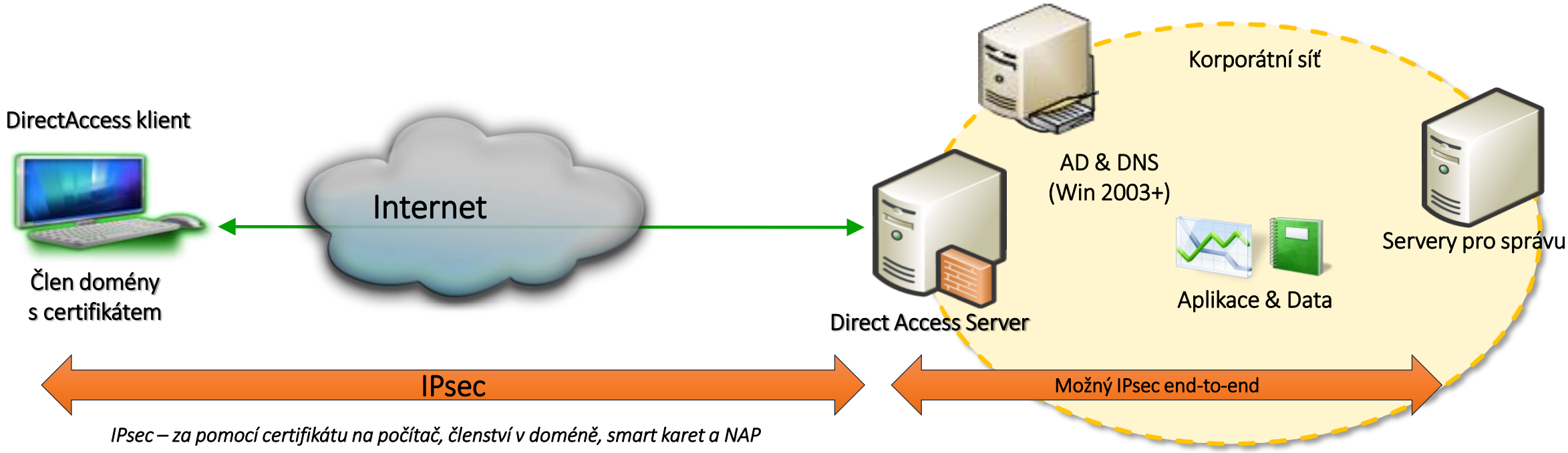
- Zabraňuje neautorizovanému přístupu k datům na ztraceném anebo ukradeném zařízení
- Podporuje šifrování systémového i/nebo datového oddílu
- Nabízí celou řadu předbootovacích autentizačních možností:
  - TPM-only, PIN/Password, Network Unlock, USB storage
- Podporuje PC, servery i tablety

BitLocker to Go

- Ochrana dat na externích přenosných discích (např. USB flash disk)
- Možnost přidělit nebo zamítnout přístup pro zápis
- Přístup pro čtení na Windows Vista & Windows XP (Bitlocker to Go Reader)

DirectAccess

Schéma zabezpečení



IPsec – za pomocí certifikátu na počítač, členství v doméně, smart karet a NAP

Security Compliance Manager

- Volně dostupný nástroj pro klienty s Windows
- Předpřipravené politiky a konfigurační balíčky založené na doporučeních Microsoft Security Guide a obecných bezpečnostních praktikách ke snadné správě zabezpečení operačního systému
- Politiky lze aplikovat prostřednictvím Group Policy a System Center Configuration Manager
- Klíčové funkce
  - Podpora všech verzí serverového a klientského OS včetně Windows 2012 a Windows 8 a Internet Exploreru
  - Referenční konfigurace (Gold Master)
  - Funguje i na počítačích mimo doménu
  - Znalostní báze bezpečnostních expertů a doporučená nastavení
  - Porovnání existujících nastavení proti doporučenému "zabezpečenému" nastavení

http://technet.microsoft.com/en-us/library/cc677002.aspx

Shrnutí

- Rozšířit strategii Risk Management u organizací „v pohybu“
- Od všeobecné ochrany interní infrastrukutry k ochraně klíčových aktiv
- Klasifikace aktiv a mapování jejich pohybu po síti organizace
- Zvolit vhodný typ klientských zařízení a architektury zabezpečení

Děkujeme

Windows