4. PŘEDNÁŠKA – CIS CONTROLS

CIS

- **Center for Internet Security Critical Security Controls for Effective Cyber Defense**
- Publikace obsahující „best practice“ v oblasti počítačové bezpečnosti
- Zdarma pro všechny
- Vytvořeno dobrovolníky ze Cyber security komunity
- Stojí na základě známých, aktuálních cyber útoků a metod
- Obsahuje 20 „Controls“ (klíčových akcí) - pro správné zabezpečení sítě

Základní CIS controls

1. Inventory and Control of Hardware Assets

2. Inventory and Control of Software Assets

3. Continuous Vulnerability Management

4. Controlled Use of Administrative Privileges

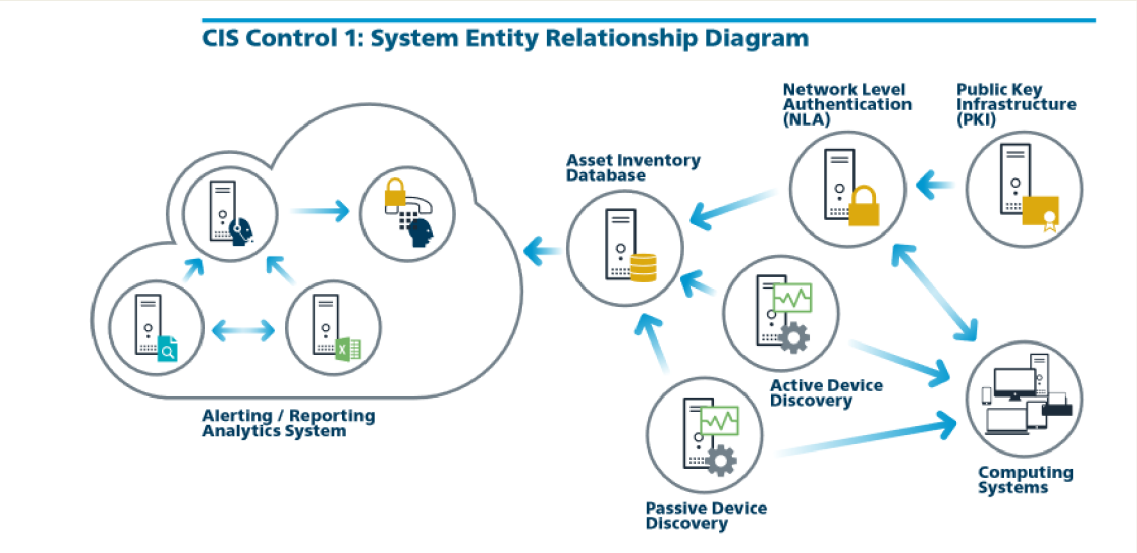
5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers

6. Maintenance, Monitoring and Analysis of Audit Logs

CIS Control 1: Inventory and Control of hardware Assets

- Inventarizace a kontrola (přehled) hardwarových aktiv

- Cíle :
  - *Aktivní správa všech HW zařízení v s*
  - *Přístupy povolit pouze autorizovaným zařízením*
  - *Nalézt neautorizovaná a nespravovan zařízení a zabránit jím v přístupu*



Důležitost CIS 1

- Útočníci neustále skenují sítě svých cílů
- Čekají na zařízení, které se připojí do sítě:
  - *nové nechráněné systémy*
  - *„Come and go off“ zařízení (Notebooky, vlastní zařízení zaměstnanců)*
  - *Nový HW (připojen ale nezabezpečen např. konfigurace a patching proběhne až další den – čas pro útočníka)*
  - *Testové systémy, demo, síť pro hosty atd…*

- Ve velkých firmách bývá problém spravovat velmi měnící se prostředí
- Správa všech zařízení hraje důležitou roli při:
  - *Plánovaní*
  - *Zálohování*
  - *Reakcích na incidenty*
  - *Zotavení po útoku*

CIS control 1: subcontrols

CIS Control 1: Inventory and Control of Hardware Assets

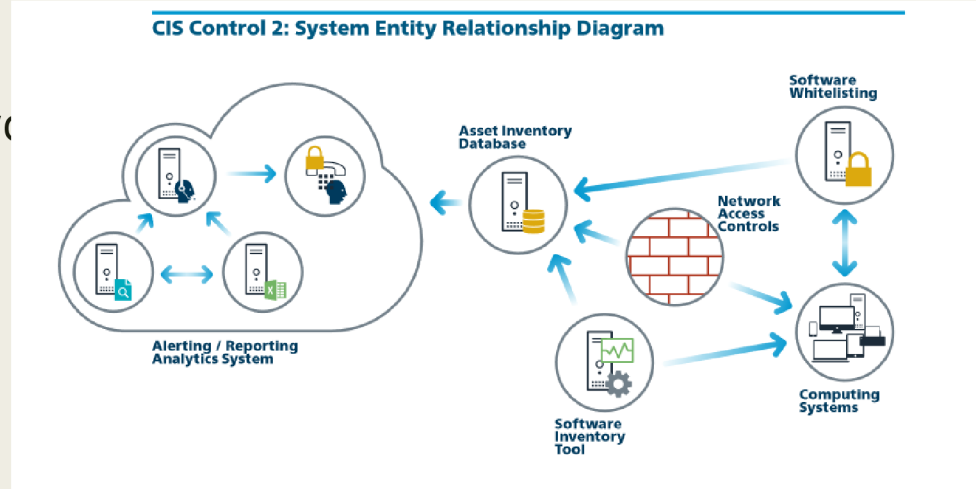
Sub-Control	Asset Type	Security Function	Control Title	Control Descriptions	Implementation Groups		
					1	2	3
1.1	Devices	Identify	Utilize an Active Discovery Tool	Utilize an active discovery tool to identify devices connected to the organization's network and update the hardware asset inventory.		●	●
1.2	Devices	Identify	Use a Passive Asset Discovery Tool	Utilize a passive discovery tool to identify devices connected to the organization's network and automatically update the organization's hardware asset inventory.			●
1.3	Devices	Identify	Use DHCP Logging to Update Asset Inventory	Use Dynamic Host Configuration Protocol (DHCP) logging on all DHCP servers or IP address management tools to update the organization's hardware asset inventory.		●	●
1.4	Devices	Identify	Maintain Detailed Asset Inventory	Maintain an accurate and up-to-date inventory of all technology assets with the potential to store or process information. This inventory shall include all assets, whether connected to the organization's network or not.	●	●	●
1.5	Devices	Identify	Maintain Asset Inventory Information	Ensure that the hardware asset inventory records the network address, hardware address, machine name, data asset owner, and department for each asset and whether the hardware asset has been approved to connect to the network.		●	●
1.6	Devices	Respond	Address Unauthorized Assets	Ensure that unauthorized assets are either removed from the network, quarantined or the inventory is updated in a timely manner.	●	●	●
1.7	Devices	Protect	Deploy Port Level Access Control	Utilize port level access control, following 802.1x standards, to control which devices can authenticate to the network. The authentication system shall be tied into the hardware asset inventory data to ensure only authorized devices can connect to the network.		●	●
1.8	Devices	Protect	Utilize Client Certificates to Authenticate Hardware Assets	Use client certificates to authenticate hardware assets connecting to the organization's trusted network.			●

CIS Control 1: Souhrn

- Udržení aktuálního a přesného přehledu = trvalý a dynamický proces
- Organizace mohou pravidelně síť skenovat pro identifikaci zařízení
- Před skenováním je potřeba zajistit dostatečnou šířku pásma (na základě historie zátěže a kapacit jejich sítě)
- Pasivní skenery pak na kritických místech sledují komunikaci na základě které se snaží identifikovat zařízení
- Informace lze získat z routerů a switchů (např. MAC adresy)
- Každé zařízení (fyzické/virtualní) využívající IP adresu by mělo být zahrnuto do inventáře aktiv organizace

CIS Control 2: Inventory and Control of Software Assets

- Inventarizace a kontrola (přehled) softwarových aktiv
- Cíle :
  - *Aktivní správa veškerého SW v síti*
  - *Povolit instalace a spuštění pouze autorizovaných SW*
  - *Nalézt neautorizované a nespravované SW a zabránit jejich instalaci a spuštění*



Důležitost CIS 2

- Útočníci neustále skenují sítě svých cílů
- Hledají zranitelné verze SW, které mohou být vzdáleně napadeny:
  - *neaktualizovaný SW*
  - *Neoprávněný SW (SW, který nemá v síti co dělat)*
  - *Nový SW (Neotestovaný v rámci bezpečnosti)*
- Bez správné znalosti a kontroly SW v organizaci nelze síť správně zabezpečit
- Útočníci rozesílají různé škodlivé weby, dokumenty, mediální soubory atd. přes důvěryhodné zdroje (Vlastní web firmy, partneři, kolegové atd)
- Využívají zero-days exploits (Využívají zranitelnosti, která ještě nemá patch)
- Po úspěšném útoku dochází k získaní kontroly nad systémem
- Špatně kontrolovatelné zařízení -> nejspíš obsahuje nepotřebný/škodlivý SW -> napadení takového zařízení = možnost napadení celé sítě ->organizace bez správy SW = nejsou schopni zjistit příčinu problému a detekovat škodlivý SW
- Správa všech SW hraje důležitou roli při:
  - *Plánovaní*
  - *Zálohování*
  - *Reakcích na incidenty*
  - *Zotavení po útoku*

CIS control 2: subcontrols

CIS Control 2: Inventory and Control of Software Assets

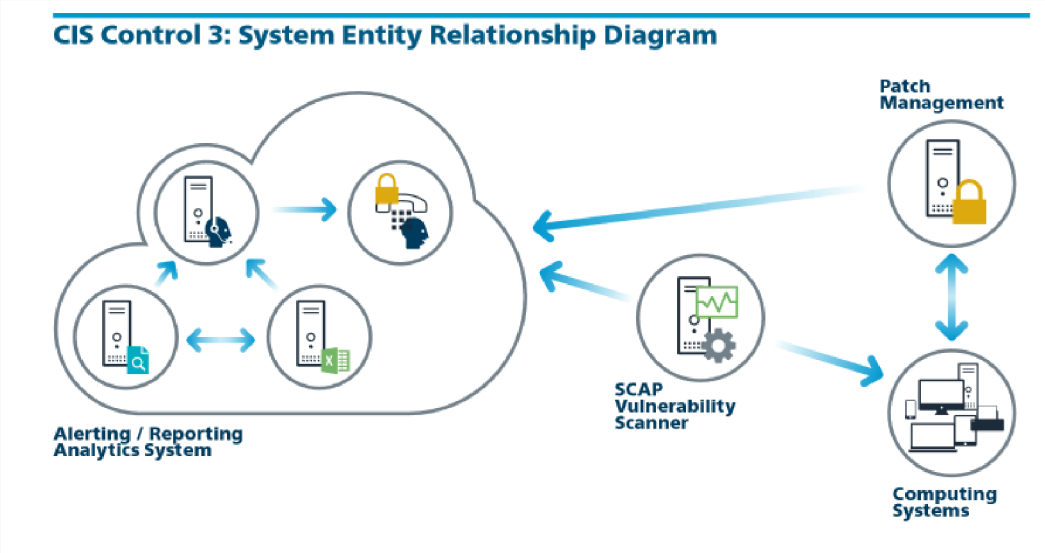
Sub-Control	Asset Type	Security Function	Control Title	Control Descriptions	Implementation Groups 1	2	3
2.1	Applications	Identify	Maintain Inventory of Authorized Software	Maintain an up-to-date list of all authorized software that is required in the enterprise for any business purpose on any business system.	●	●	●
2.2	Applications	Identify	Ensure Software Is Supported by Vendor	Ensure that only software applications or operating systems currently supported and receiving vendor updates are added to the organization's authorized software inventory. Unsupported software should be tagged as unsupported in the inventory system.	●	●	●
2.3	Applications	Identify	Utilize Software Inventory Tools	Utilize software inventory tools throughout the organization to automate the documentation of all software on business systems.		●	●
2.4	Applications	Identify	Track Software Inventory Information	The software inventory system should track the name, version, publisher, and install date for all software, including operating systems authorized by the organization.		●	●
2.5	Applications	Identify	Integrate Software and Hardware Asset Inventories	The software inventory system should be tied into the hardware asset inventory so all devices and associated software are tracked from a single location.			●
2.6	Applications	Respond	Address Unapproved Software	Ensure that unauthorized software is either removed or the inventory is updated in a timely manner.	●	●	●
2.7	Applications	Protect	Utilize Application Whitelisting	Utilize application whitelisting technology on all assets to ensure that only authorized software executes and all unauthorized software is blocked from executing on assets.			●
2.8	Applications	Protect	Implement Application Whitelisting of Libraries	The organization's application whitelisting software must ensure that only authorized software libraries (such as *.dll, *.ocx, *.so, etc.) are allowed to load into a system process.			●
2.9	Applications	Protect	Implement Application Whitelisting of Scripts	The organization's application whitelisting software must ensure that only authorized, digitally signed scripts (such as *.ps1,*.py, macros, etc.) are allowed to run on a system.			●
2.10	Applications	Protect	Physically or Logically Segregate High Risk Applications	Physically or logically segregated systems should be used to isolate and run software that is required for business operations but incurs higher risk for the organization.			●

CIS Control 2: Souhrn

- Whitelisting lze implementovat pomocí kombinace komerčních whitelistingových nástrojů, zásad (policy) a nástrojů testující aplikace, které přicházejí společně s antivirovými balíčky a populárními operačními systémy.
- Komerční nástroje pro inventarizaci SW a zařízení jsou dnes široce dostupné a používají se v mnoha podnicích.
- Nejlepší nástroje poskytují kontrolu stovek běžných aplikací používaných v podnicích
- Získávají informace o dostupných patch-ích.
- Komerční nástroje navíc stále více sdružují antiviry, antispyware, osobní brány firewall, IDS, IPS spolu s bílou a černou listinou aplikací.

CIS Control 3: Continuous Vulnerability Management

- Aktivní správa zranitelností
- Zranitelnost (Vulnerability) = V počítačové bezpečnosti je zranitelností slabost, kterou může útočník, zneužít k provádění neoprávněných akcí v počítačovém systému.
- Cíle :
  - *Neustále získávat a vyhodnocovat nové informace, které vedou k:*
    - Identifikaci zranitelností
    - Nápravě (remediate)
    - Minimalizaci příležitostí pro útočníky (attack surface)



Důležitost CIS 3

- Správa zranitelností je trvalá aktivita vyžadující čas, pozornost a zdroje
- Bezpečnostní týmy musí pracovat se spoustu neustálých informací (aktualizace SW, patch, bezpečnostní doporučení atd.)
- Útočníci mají přístup ke stejným informacím ohledně zranitelností, kterých můžou využít
- Nahlášena nová zranitelnost -> závod mezi: útočníky (Co nejrychleji zneužít), prodejci (Co nejrychleji vydat patch, aktualizaci) a bezpečnostních týmů(vyhodnocování rizik, instalace patchů)
- Organizace, které neřeší zranitelnosti čelí velké pravděpodobnosti ohrožení jejich počítačových systémů
- V takových organizacích je remedeation (nápravné opatření) velice obtížné

CIS control 3: subcontrols

CIS Control 3: Continuous Vulnerability Management

Sub-Control	Asset Type	Security Function	Control Title	Control Descriptions	Implementation Groups		
					1	2	3
3.1	Applications	Detect	Run Automated Vulnerability Scanning Tools	Utilize an up-to-date Security Content Automation Protocol (SCAP) compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.		●	●
3.2	Applications	Detect	Perform Authenticated Vulnerability Scanning	Perform authenticated vulnerability scanning with agents running locally on each system or with remote scanners that are configured with elevated rights on the system being tested.		●	●
3.3	Users	Protect	Protect Dedicated Assessment Accounts	Use a dedicated account for authenticated vulnerability scans, which should not be used for any other administrative activities and should be tied to specific machines at specific IP addresses.		●	●
3.4	Applications	Protect	Deploy Automated Operating System Patch Management Tools	Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.	●	●	●
3.5	Applications	Protect	Deploy Automated Software Patch Management Tools	Deploy automated software update tools in order to ensure that third-party software on all systems is running the most recent security updates provided by the software vendor.	●	●	●
3.6	Applications	Respond	Compare Back-to-Back Vulnerability Scans	Regularly compare the results from consecutive vulnerability scans to verify that vulnerabilities have been remediated in a timely manner.		●	●
3.7	Applications	Respond	Utilize a Risk-Rating Process	Utilize a risk-rating process to prioritize the remediation of discovered vulnerabilities.		●	●

CIS Control 3: Souhrn

- Existuje velké množství nástrojů, pro skenovaní zranitelností
- Pro standardizovaní odhalených zranitelností je lepší využívat skeny, které využívají: CVE, CCE, OVAL, CPE, CVSS a / nebo XCCD
- Pokročilé nástroje lze nakonfigurovat s přihlašovacími údaji pro provádění komplexnějších prohledávání, než jaké lze dosáhnout bez přihlašovacích údajů.
- Nástroje také mohou kontrolovat nastavení jednotlivých zařízení
- Nástroje lze propojit s ticket systémy
- Nástroje porovnávají jednotlivé skeny = vytváření reportů a trendů

Seminář

iTop

- https://www.combodo.com/teemip-online-demo

Qualys

- Qualys community edition
- https://www.qualys.com/community-edition/

CIS benchmark

- Cis-cat-full.zip

Nikto

- https://github.com/sullo/nikto

zdroje

- https://www.cisecurity.org/