

**PROVÁDĚJTE HARDENING KONFIGURACE SERVEROVÝCH APLIKACÍ**  
tj. databází, webových aplikací, CRM systémů, účetních systémů, HR systémů a dalších systémů ukládání dat.

#### KONTROLUJTE PŘENOSNÁ MÉDIA

jako součást širší strategie prevence ztráty dat, včetně vedení seznamu povolených USB zařízení, jejich skladování, šifrování, mazání a likvidace.

**OMEZTE PŘÍSTUP K SERVER MESSAGE BLOCKU (SMB) A NETBIOSU**  
na pracovních stanicích a serverech, kdekoliv je to možné.

**POUŽÍVEJTE REŽIM CHRÁNĚNÉHO PŘÍSTUPU PŘI PRÁCI SE SOUBORY NA ÚROVNI PRACOVNÍCH STANIC**

může se např. jednat o Protected View nebo Protected mode.

#### VYNUȚTE VYTÁČENÍ VPN,

pokud se zařízení připojuje mimo síť organizace. Omezte síťovou aktivitu, dokud není navázáno VPN spojení.

#### ZAJISTĚTE FYZICKOU BEZPEČNOST IT TECHNIKY



#### SPRÁVA ÚČTŮ



#### ZAVEĎTE CENTRÁLNÍ SPRÁVU UŽIVATELSKÝCH ÚČTŮ A OPRÁVNĚNÍ

a nastavte jednotnou bezpečnostní politiku. Účtům, u kterých to není vyžadováno, odeberte rozšířená oprávnění a zakažte spouštění skriptů, instalaci softwaru, úpravy registru atd.

#### VYNUCUJTE VÍCEFAKTOROVOU AUTENTIZACI

zejména pro akce vyžadující vyšší úroveň oprávnění a kritické operace jako vzdálený přístup nebo přístup k citlivým informacím.

#### ODDĚLITE ADMINISTRÁTORSKÉ ÚČTY

Pro správu používejte speciální účty pro administraci systémů. Pro své ostatní pracovní aktivity (e-mail, web atd.) používejte běžný neprivilegovaný účet. Účet s oprávněním doménového administrátora je použit pouze ke správě Domain Controlleru (tzn. nepřistupuje na klientské stanice a servery).

#### PŘIDĚLTE KAŽDÉMU ADMINISTRÁTOROVI VLASTNÍ ÚČET

pro správu systémů. Nepoužívejte sdílené účty.

#### ZABEZPEČTE LOKÁLNÍ ADMINISTRÁTORSKÉ ÚČTY.

Nastavte unikátní heslo na každě stanici, v prostředí Windows můžete využít například LAPS (Local Administrator Password Solution).

#### VYNUȚTE POUŽIVÁNÍ SILNÝCH HESEL

s ohledem na vyžadovanou složitost, délku a dobu platnosti. Zamezte opakovanému použití stejných hesel a používání slovníkových výrazů. Vynuťte změnu hesla, existuje-li podezření, že bylo kompromitováno.

**PROVIDELNĚ KONTROLUJTE UŽIVATELSKÉ ÚČTY A JEJICH OPRÁVNĚNÍ**  
a to jak lokální, tak centrálně spravované.

# BEZPEČNOSTNÍ DOPORUČENÍ NÚKIB PRO ADMINISTRATORY 4.0



#### INFRASTRUKTURA



#### ČLEŇTE SÍŤ NA MENŠÍ CELKY (SEGMENTACE) A STRIKTNĚ ODDĚLUJTE UŽIVATELSKÁ PRÁVA NAPŘÍČ UŽIVATELI (SEGREGACE)

s cílem oddělit citlivé informace a kritické služby typu autentizace uživatelů (např. Microsoft Active Directory) a vytvořit zóny s různou úrovní bezpečnostních omezení.

#### BLOKUJTE ŠKODLIVÉ IP ADRESY A DOMÉNY NA ÚROVNI GATEWAY (BLACKLISTY).

#### NASAĎTE SÍŤOVÉ SYSTÉMY DETEKCE / PREVENCE PRŮNIKU (IDS/IPS)

používající signatury a heuristiky k identifikaci anomálního provozu v rámci sítě i překračujícího perimetru.

#### SLEDUJTE SÍŤOVÝ PROVOZ

pomocí vybraných síťových prvků nebo rozmístění dedikovaných síťových sond. Sledujte komunikaci mezi klienty a servery, komunikaci klientů do internetu, komunikaci mezi servery i provoz na perimetru sítě a identifikujte provozní a bezpečnostní problémy.

#### UCHOVÁVEJTE SÍŤOVÝ PROVOZ

z/do kritických pracovních stanic a serverů a provoz překračující perimetru pro případné forenzní zkoumání po průniku do sítě a systémů. Záznamy síťového provozu doporučujeme uchovávat po dobu minimálně 12 měsíců, více podle místních okolností a významu sítě – v případě kritické informační infrastruktury (KII) a u informačních systémů základní služby (PZS) podle zákona o kybernetické bezpečnosti a návazných vyhlášek je minimální lhůta 18 měsíců. V případě sítí strategického významu zvažte i možnost automaticky aktivovaného plného záznamu datového provozu (PCAP), a to jak na primárních, tak záložních systémech (např. webových nebo systémových serverech).

#### KONTROLUJTE PŘÍCHOZÍ E-MAILY

pomocí mechanismů Sender ID, SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail) a DMARC (Domain-based Message Authentication, Reporting and Conformance) a blokujte podvržené zprávy. Tyto mechanismy nastavte i pro možnou kontrolu odchozích zpráv druhou stranou.

#### POUŽÍVEJTE ŠIFROVANÉ SPOJENÍ MEZI POŠTOVNÍMI SERVERY (TLS)

pro zajištění důvěrnosti e-mailové komunikace, v ideálních případech použijte DANE (DNS-based Authentication of Named Entities). Kontrolu obsahu provádějte až poté, co je e-mailový provoz dešifrován.

#### PROVÁDĚJTE AUTOMATIZOVANOU DYNAMICKOU ANALÝZU OBSAHU E-MAILŮ A WEBŮ

prováděnou v sandboxu – hledejte podezřelé chování podle síťového provozu, tvorby nových souborů, úpravy stávajících souborů nebo změn konfigurace.

#### POVOLTE NA FIREWALLU POUZE ŽÁDOUCÍ SLUŽBY A STANDARDNÍ PROVOZ.

V případě koncových stanic nezapomeňte také blokovat spojení z Vámi nekontrolované sítě.

#### KONTROLUJTE POUŽÍVANÉ KLÍČE/CERTIFIKÁTY

především pro SSH autentizaci, webové servery, vzdálenou plochu apod. Kde je to možné, použijte šifrovanou komunikaci.



## ZAJISTĚTE CENTRALIZOVANÉ A ČASOVĚ SYNCHRONIZOVANÉ LOGOVÁNÍ SÍŤOVÝCH UDÁLOSTÍ

(povolených a blokovaných) s okamžitým automatickým vyhodnocováním a uložením po dobu minimálně 18 měsíců, více podle místních okolností a významu sítě.

## APLIKUJTE WHITELISTING WEBOVÝCH DOMÉN

pro všechny domény – pokud to dovoluje charakter práce uživatelů. Tento přístup je účinnější než blacklistovat malé procento škodlivých domén.

## VOLTE JEDNODUCHÉ DOMÉNOVÉ NÁZVY,

aby byly jasné viditelné případné záměny písmen ve phishingových e-mailech.

## NASAĎTE ANTI-DDoS TECHNOLOGIE,

které můžete po důkladné úvodní analýze řešit buď vlastními silami, nebo ve spolupráci s poskytovatelem internetového připojení. Anti DDoS ochranu nasadte na kompletní IP rozsahy vaší organizace.

## VYPRACUJTE DISASTER RECOVERY PLAN (DRP)

a mějte připravené správné a funkční emailové adresy a telefonní čísla na ostatní administrátory, nadřízené pracovníky a CERT/CSIRT týmy.



## STANICE A SERVERY



### UDRŽUJTE AKTUÁLNÍ OPERAČNÍ SYSTÉM

pravidelnými aktualizacemi a v co nejkratší době aplikujte všechny vydané bezpečnostní záplaty.

### UDRŽUJTE AKTUÁLNÍ SOFTWARE,

pravidelně kontrolujte verze instalovaného softwaru. U neaktuálního softwaru provedte v rámci možností update. Zastaralé mohou být i verze použitých doplňků či modulů nebo firmware zařízení.

### NEPOUŽIVEJTE NEPODPOROVANÉ PRODUKTY,

používejte pouze produkty (software i operační systémy), pro které jsou dostupné bezpečnostní záplaty.

### OVĚŘUJTE IDENTITU APLIKACÍ A SOUBORŮ

a povolte jen ty důvěryhodné včetně skriptů a DLL knihoven. V prostředí Windows použijte Device Guard, AppLocker, popřípadě Zásady omezení softwaru (SRP).

### PROVÁDĚJTE HARDENING KONFIGURACE UŽIVATELSKÝCH APLIKACÍ

– povolte jen funkcionality, která je vyžadována pro práci uživatelů. Dodatečné funkce (např. Java a Flash ve webovém prohlížeči, makra v MS Office) povolte pouze, je-li to nutné.

### POUŽIVEJTE OBECNÉ PREVENTIVNÍ MECHANISMY,

které mohou pomoci ochránit systém před zero-day zranitelnostmi, jako např. DEP (Data Execution Prevention) nebo SELinux v linuxových systémech.

### AKTIVUJTE IDS/IPS SYSTÉMY NA KONCOVÝCH STANICích

detekující anomální chování jako např. injekci kódu do jiných procesů, změnu chráněných registrůvých klíčů, zachytávání stisků kláves, načítání neznámých ovladačů, snahu o zajištění perzistence a další.

## ZAJISTĚTE CENTRALIZOVANÉ A ČASOVĚ SYNCHRONIZOVANÉ LOGOVÁNÍ SÍŤOVÝCH UDÁLOSTÍ

(povolených a blokovaných) s okamžitým automatickým vyhodnocováním a uložením pro kritickou informační infrastrukturu (KII) a provozovatele základní služby (PZS) po dobu minimálně 18 měsíců, pro významné informační systémy (VIS) po dobu minimálně 12 měsíců a pro ostatní systémy podle místních okolností a významu sítě.

### FILTRUJTE OBSAH E-MAILŮ A PROPOUŠTĚJTE POUZE RELEVANTNÍ DRUHY PŘÍLOH

– po důkladné analýze chování uživatelů určete typy souborů, které potřebují posílat e-mailem. Ostatní formáty přílohy blokuje – především spustitelný kód. Dále ověřujte soulad přípony souboru a jeho skutečného formátu.

### PRAVIDELNĚ ZÁLOHUJTE DŮLEŽITÁ A CITLIVÁ DATA

jako např. obsah webového serveru, databází nebo konfiguraci služeb. Zálohu umístěte do odděleného prostředí mimo produkční síť. Pravidelně testujte, jestli dokážete data obnovit a jestli jsou data po obnově funkční.

### ZAVEĎTE STANDARD OPERATING ENVIRONMENT (SOE)

se standardizovanou konfigurací pro pracovní stanice i servery, kde budou vypnuty všechny nevyžádané funkcionality.

### ZAMEZTE PŘÍMÉMU PŘÍSTUPU PRACOVNÍCH STANIC NA INTERNET

a směrujte provoz přes split DNS server, e-mailový server nebo autentizovaný web proxy server. Nezapomeňte vynutit pro IPv4 i IPv6.

### POUŽÍVEJTE ANTIWIROVÝ A BEZPEČNOSTNÍ SOFTWARE

a nástroje, které zakazují spouštění nebezpečných aplikací (mimo přesně definovaný seznam privilegovaných aplikací), či nástroje, které pomáhají chránit systém v době, kdy nejsou dostupné klasické bezpečnostní aktualizace.

### ŠIFRUJTE DISKY

– zejména u přenosných počítačů – včetně centrální evidence klíčů.

### VYUŽÍVEJTE TRUSTED PLATFORM MODULE (TPM),

tedy zabezpečený kryptografický modul pro generování a uložení hesel a kryptografických klíčů, je-li jím počítač vybaven.

### NASTAVTE HESLO UEFI / BIOS

unikátní pro každou stanici s centrální správou hesel.

### VYNUCUJTE SECURE BOOT

a nastavte pořadí zařízení určených pro boot systému. Boot manager musí být zabezpečen heslem.

### CHRAŇTE SE PŘED ÚTOKY NA HESLA

u všech služeb, kam se přihlašují uživatelé. Například pomocí fail2ban, využití funkcí určených pro ukládání hesel (Argon2, bcrypt, scrypt, PBKDF2) nebo CAPTCHA.

### PRO SPRÁVU SERVERŮ POMOCÍ SSH VYUŽÍVEJTE PRO PŘIHLÁŠENÍ KLÍČE, ZAKAŽTE HESLA

Pro svázání otisku klíče se serverem, kde je použitý, využívejte SSHFP záznamy v DNS ideálně v kombinaci s DNSSEC, který zajistí autenticitu odpovědi obsahující SSHFP záznam.