BEZPEČNOSTNÍ DOPORUČENÍ NCKB

INFRASTRUKTURA

AUTOMATIZOVANÁ DYNAMICKÁ ANALÝZA
obsahu e-mailů a webu prováděná v sandboxu, ve kterém je možné pozorovat podezřelé chování podle: síťového provozu, tvorby nových souborů, úpravy stávajících souborů nebo změn konfigurace.

ČLENĚNÍ SÍTĚ NA MENŠÍ CELKY (SEGMENTACE) A STRIKTNÍ ODDĚLOVÁNÍ UŽIVATELSKÝCH PRÁV NAPŘÍČ UŽIVATELI (SEGREGACE)
Cílem je oddělení citlivých informací a kritických služeb typu autentizace uživatelů (např. Microsoft Active Directory) a vytvoření zón s různou úrovní bezpečnostních omezení.

SOFTWAROVÝ APLIKAČNÍ FIREWALL BLOKUJÍCÍ NESTANDARDNÍ PŘÍCHOZÍ PROVOZ
V případě koncových stanic také blokující spojení iniciovaná jinou stranou.

SOFTWAROVÝ APLIKAČNÍ FIREWALL BLOKUJÍCÍ ODCHOZÍ PROVOZ
pocházející od jiných než whitelistovaných aplikací, zabraňující jakémukoliv neznámému odchozímu provozu.

VIRTUALIZOVANÉ PROSTŘEDÍ FORMOU JEDNORÁZOVÉHO SANDBOXU
hostované mimo interní síť organizace, určené pro rizikové aktivity jako surfování po internetu.

CENTRALIZOVANÝ A ČASOVĚ SYNCHRONIZOVANÝ SYSTÉM LOGOVÁNÍ SÍŤOVÝCH UDÁLOSTÍ
(povolených a blokovaných) s okamžitým automatickým vyhodnocováním a uložením po dobu minimálně 18 měsíců.

FILTR OBSAHU WEBOVÝCH STRÁNEK PRO PŘÍCHOZÍ I ODCHOZÍ PROVOZ
s whitelistem povolených druhů webového obsahu a používající behaviorální analýzu, externí reputační žebříčky, heuristiku a signatury.

WHITELISTING WEBOVÝCH DOMÉN PRO VŠECHNY DOMÉNY
Tento přístup je důkladnější a účinnější než blacklistovat malé procento škodlivých domén.

BLOKOVÁNÍ PODVRŽENÝCH E-MAILŮ
používáním Sender ID nebo Sender Policy Framework (SPF) pro kontrolu příchozích e-mailů, a 'hard-fail' nastavení SPF záznamu, které pomůže ochránit podvržení domény vaší organizace a u většiny mailových klientů označí příchozí zprávu jako spam.

TLS ŠIFROVÁNÍ MEZI MAILOVÝMI SERVERY
pro minimalizaci možnosti zachycení legitimních e-mailů a jejich zneužití pro sociální inženýrství. Provádějte kontrolu obsahu poté, co je emailový provoz dešifrován.

SÍŤOVÉ SYSTÉMY DETEKCE / PREVENCE PRŮNIKU (IDS/IPS)
používající signatury a heuristiku k identifikaci anomálního provozu v rámci sítě i překračujícího perimetr.

BLACKLISTY NA ÚROVNI GATEWAY SERVERU
blokující přístup ke známým škodlivým IP adresám a doménám, včetně dynamických a jiných domén poskytovaných zdarma anonymním uživatelům internetu.

UCHOVÁVAT SÍŤOVÝ PROVOZ
z/do kritických pracovních stanic a serverů a provoz překračující perimetr sítě pro případné forenzní zkoumání po průniku do sítě a systémů.

VYBUDOVÁNÍ DRP (DISASTER RECOVERY PLAN)
včetně získání nebo kontroly správnosti e-mailové adresy, telefonního čísla aj. na CERT/CSIRT týmy, nadřízené pracovníky a ostatní administrátory.

KONTROLA CERTIFIKÁTŮ
Proveďte kontrolu použitých certifikátů. Certifikáty pro SSH autentizaci, pro webové servery, pro vzdálenou plochu apod. Pokud je to možné, vždy využijte šifrované komunikace.

STANICE & SERVERY

IDENTITA APLIKACÍ A SOUBORŮ
Povolte jen ověřené a důvěryhodné aplikace a soubory (včetně skriptů a dll knihoven). Ve Windows sítích použijte Applocker popřípadě Zásady omezení softwaru (SRP).

AKTUÁLNÍ SOFTWARE
Zkontrolujte verze instalovaného softwaru. U neaktuálního softwaru proveďte v rámci možností update. Zastaralé mohou být i verze použitých doplňků či modulů.

AKTUÁLNÍ OPERAČNÍ SYSTÉM
Pravidelně provádějte aktualizace operačního systému a aplikujte všechny vydané bezpečnostní záplaty v co nejkratší době. Používejte pouze verze s podporou.

HARDENING KONFIGURACE UŽIVATELSKÝCH APLIKACÍ
Povolte pouze funkcionalitu, která je vyžadována. Dodatečné funkce (např. Java a Flash ve webovém prohlížeči, makra v MS Office) povolte pouze, je-li to nutné.

OBECNÉ PREVENTIVNÍ MECHANISMY V OPERAČNÍM SYSTÉMU
které mohou pomoci chránit systémy před 0-day zranitelnostmi, např. Microsoft EMET, DEP (Data Execution Prevention), ASLR (Address Space Layout Randomization) nebo SELinux v linuxových systémech.

IDS/IPS PROVOZOVANÉ NA KONCOVÉ STANICI
detekující anomální chování, jako např. injekce kódu do jiných procesů, změny chráněných registrových klíčů, zachytávání stisků klávesnice, načítání neznámých ovladačů, udržení přístupu.

CENTRALIZOVANÝ A ČASOVĚ SYNCHRONIZOVANÝ SYSTÉM LOGOVÁNÍ
událostí v počítačích (úspěšných i neúspěšných) s okamžitým automatickým vyhodnocováním a uložením po dobu minimálně 18 měsíců.

FILTR OBSAHU E-MAILŮ PROPOUŠTĚJÍCÍ POUZE RELEVANTNÍ DRUHY PŘÍLOH
Pokud možno s analýzou/konverzí/ošetřením odkazů a příloh ve formátech PDF nebo MS Office. Zamezte doručování formátů, které nejsou nutné (scr, exe, dll atd.).

PRAVIDELNĚ PROVÁDĚJTE ZÁLOHOVÁNÍ DŮLEŽITÝCH A CITLIVÝCH DAT
jako např. obsah webového serveru, databází nebo nastavení služeb. Také pravidelně testujte, že zálohy jsou funkční a je možné z nich data obnovit.

SPRÁVA KONFIGURACE PRACOVNÍCH STANIC A SERVERŮ
postavená na standardním operačním prostředí (SOE - Standard Operating Environment), kde jsou vypnuty všechny nevyžádané funkcionality, např. IPv6, autorun a LanMan.

ZAMEZENÍ PŘÍMÉHO PŘÍSTUPU PRACOVNÍCH STANIC NA INTERNET
tak, aby byl provoz směrován přes split DNS server, e-mailový server nebo autentizovaný web proxy server. Nezapomeňte toto vynutit v IPv4 i v IPv6.

POUŽITÍ ANTIVIROVÉHO A BEZPEČNOSTNÍHO SOFTWARU
Používejte antivirový software a nástroje, které zakazují spouštění nebezpečných aplikací (definován seznam privilegovaných aplikací), či nástroje, které pomáhají chránit systém v době, kdy nejsou dostupné klasické bezpečnostní aktualizace.

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

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

HLEDÁNÍ POTENCIÁLNĚ ŠKODLIVÝCH ANOMÁLIÍ V DOKUMENTECH MICROSOFT OFFICE NA ÚROVNI PRACOVNÍCH STANIC
tj. používání Microsoft Office File Validation nebo karantény Protected View.

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

KONTROLA NAPLÁNOVANÝCH AKCÍ A SLUŽEB PO STARTU SYSTÉMU
Škodlivý kód nemusí být spuštěn ihned, ale může se nacházet v předem naplánovaných úlohách (plánovač úloh, cron, registry atd.).

UŽIVATELÉ

VÍCEFAKTOROVÁ AUTENTIZACE
Vynucujte vícefaktorovou autentizaci pro kritické operace (vzdálený přístup, akce vyžadující vyšší úroveň oprávnění, přístup k citlivým informacím).

ODDĚLENÍ ADMINISTRÁTORSKÝCH ÚČTŮ
Jako správce používejte speciální účet pro administraci systémů. Pro ostatní aktivity (e-mail, web atd.) používejte běžný neprivilegovaný účet.

POLITIKA SILNÉHO HESLA
S ohledem na vyžadovanou složitost, délku a dobu platnosti. Zamezte opakovanému použití stejných hesel a používání slovníkových výrazů. Vynuťte změnu hesla, pokud bylo kompromitováno.

KONTROLA UŽIVATELSKÝCH ÚČTŮ A JEJICH OPRÁVNĚNÍ
Pravidelně kontrolujte uživatelské účty (lokální i centrálně spravované). Nastavte bezpečnostní politiku pro účty a odeberte účtům, u kterých to není vyžadováno, rozšířená oprávnění (zákaz spouštění skriptů, zákaz instalace softwaru, úpravy registru).