GYTPOL

Produktový list

Gytpol Validator

Zneužívání konfiguračních chyb pro obcházení ochranných mechanismů je běžnou praxí útočníků. Riziková nastavení však stále nejsou v hledáčku konvenčních bezpečnostních nástrojů a manuální adresování dané problematiky pak přináší řadu výzev i pro rozsáhlé IT týmy. Identifikace zranitelných konfigurací vyžaduje mimořádně širokou znalostní bázi zahrnující best practices výrobců daných systémů, pochopení hardening frameworků a komplexní přehled o využívání jednotlivých systémů. Samotná identifikace miskonfigurací je ovšem pouze drobným krůčkem k řešení – jejich úprava mnohdy vede ke znefunkčnění některých systémů, procesů či aplikací se závislostí na daném jevu. Pokud vezmeme v potaz i historická nastavení – faktor lidského pochybení či všudypřítomný nedostatek personálních kapacit – pak se z manuálního hardeningu stává nerealizovatelný projekt. Gytpol Validator je unikátní, ucelená platforma pro detekci konfiguračních chyb a automatizaci hardeningu.

Detekce

Validator ke svému fungování využívá hlavní 2 prvky. Gytpol Server obstará načítání dat z napojených systémů a dokáže tak identifikovat riziková nastavení či konfigurační chyby v rámci AD, GPo a M365. Druhou, pro obdobně zaměřené nástroje unikátní komponentou je Gytpol Agent – jeho nasazením na koncové body (Windows, Windows Server, Linux, MacOS) zajistíme real-time visibilitu do stavu konfigurací a případných nesouladech vůči centrálně prosazované baseline. Právě tyto nesoulady a chyby propsání konfigurace jsou nejfrekventovanějším typem nálezu a vzhledem ke svému charakteru nejsou detekovatelné jinými technologiemi. Kromě odchylek pak agent detekuje i další problémy na rovině koncových bodů – Cachovaná cleartextová hesla, nežádoucí lokální konfigurace či připojení k nezabezpečeným WiFi.

Klíčové charakteristiky

- Jediná technologie svého druhu
- Nasazení a zprovoznění do 2 hodin
- Dostupné on-premise či v cloudu
- Kontinuální dohled nad konfiguracemi AD, GPo, Windows, Windows Server, Linux i MacOS
- Detekce miskonfigurací na základě široké knihovny zranitelných nastavení
- Benchmarking stavu proti CIS, NIST a CyberEssentials
- Automatizace náprav nálezů včetně prověření dopadu na funkčnost
- Rollback nápravných opatření
- Možnost permaneního zapečetění vybraných nastavení
- Usnadnění komplexního konfiguračního hardeningu do řádu týdnů, nikoliv let
- Dohledání nepropsaných GPo
- Identifikace neopravitelných zranitelností
- Detekce rizikových defaultních nastavení

Práce s nálezy

Souhrn všech nálezů je kategorizován dle závažnosti, oblasti výskytu (počítače, servery, doménové řadiče, Active Directory), možných dopadů a zneužitelnosti (lateral movement, eskalace oprávnění, zneužití přihlašovacích údajů či další) či dle rozporů s compliance šablonami.

Jednotlivé nálezy jsou opatřeny podrobným popisem chyby, možností exploitace a doporučením postupu manuální nápravy. V případě false positive, resp. rizikové konfigurace jejíž změna není možná lze jev z reportingu vyjmout.

Přehled nálezů je denně aktualizován a detekční soubor se s každým dalším releasem rozšiřuje. Gytpol je v průběhu posledních let velmi rychlý v reakcích a doplnění nápravných opatření na nové hrozby, jako Follina, Log4J, PrintNightmare a další – možnosti detekce i nápravy byly doplněny updatem v řádu dní od objevení.

Automatizace náprav

Manuální opravy miskonfigurací jsou mimořádně časově i znalostně náročný proces. Vyžadují důsledné prozkoumání možných dopadů změn – zakázání některých funkcionalit může často vést ke znefunkčnění na nich závislých systémů.

Gytpol tuto oblast sofistikovaně automatizuje – Přímo z přehledného GUI umožní u jednotlivých nálezů iniciovat opravu na pár kliknutí. Při konfiguraci nápravy poskytne možnost aplikovat proces na jednotlivá zařízení, skupiny či plošně. Zohledňuje při tom informace získané monitorováním využití daných jevů a předchází tak omezení provozu.

V případě selhání je dále možné využít funkci rollback, která provedené úkony vrátí do původního stavu.