INFORMATION GATHERING

Internet v dnešní době poskytuje rozsáhlý zdroj informací o každé organizaci. Některé informace mohou být zneužity pro kybernetický útok, pokud je útočník využije ve svůj prospěch na úkor bezpečnosti dané organizace. Dohledatelná data z veřejně dostupných zdrojů pro Vás vytváří riziko digitální stopy.

Služba **Information Gathering (IG)** přestavuje komplexní vstupní informační analýzu o Vaší organizaci, která vzniká nad veřejně dostupnými informacemi, a to z volně dostupných zdrojů v prostředí internetu (vč. darknetu, soc. sítí, ...). Taková vstupní informační analýza nabízí přehled informací o Vás a Vaší organizaci, které se volně „potulují" internetem, a pomůže tak zjistit kritické oblasti, které mohou být cílem kybernetického útoku. Únik citlivých informací může v dnešní době představovat zásadní riziko, které ohrožuje dobrou pověst a bezpečnost Vaší společnosti.

Sami uvidíte, jaké informace jsou si o Vás potenciální útočníci (hackeři) schopni velmi rychle zjistit, jaké Vaše slabé stránky jsou schopni identifikovat, a snadno je tak zneužít ke kybernetickému útoku. Výsledky této informační analýzy identifikují cíle pro zvýšení kybernetické bezpečnosti a pomohou Vaší organizaci zvolit správné nástroje pro zabezpečení cílových systémů a sítí.

V rámci poskytování služby IG využíváme především nástroje OSINT (Open-source inteligence):

- Automatizované nástroje, které mohou provádět celosvětové skenování během několika minut.
- Přizpůsobitelné nástroje, které dokážou odfiltrovat irelevantní výsledky pomocí vyhledávacích kritérií.
- Systémy, které umožňují dotazovat se na data z jednotlivých zařízení (IT, OT, IoT)
- Investigativní nástroje, které zjišťují relevantní informace související s předmětem zájmu.
- Nástroje, o kterých je známo, že je používají hackeři.
- Nástroje, které jsou používané v oblasti kybernetické bezpečnosti.

VLASTNÍ POSKYTOVÁNÍ SLUŽBY IG ROZDĚLUJEME DO 5 KROKŮ:

1. **IDENTIFIKACE CÍLE NEBO CÍLŮ**
   Prvním krokem je analýza organizace. Pro větší organizace možnost zaměření se jen na dohodnuté cíle či části.
2. **IDENTIFIKACE ZDROJŮ INFORMACÍ A SBĚR DAT**
   Druhým krokem je identifikace různých nástrojů a technik, které budou použity pro sběr informací o cíli. Tento krok umožňuje útočníkům získat co nejvíce informací o cíli.
3. **FILTROVÁNÍ DAT**
   Třetí krok pomáhá filtrovat data a převádět je na smysluplné a použitelné informace.
4. **ANALÝZA**
   Čtvrtý krok kombinuje informace z více zdrojů.
5. **HLÁŠENÍ**
   Pátý krok je reportování klientovi. Informace s podrobnostmi o rizicích a jejich zmírnění.

SLUŽBA INFORMATION GATHERING

Základní funkcí testů je pomáhat týmům IT specialistů objevit veřejně přístupná aktiva a mapovat, jaké informace by se snadno mohly stát terčem potenciálního útoku.

Následně se testy využívají pro analýzu, kde jsou jednotlivé zranitelnosti aplikací, serverů, infrastruktury atp.

V RÁMCI POSKYTOVÁNÍ SLUŽBY IG SE VĚNUJEME PŘEDEVŠÍM TĚMTO ZÁKLADNÍM OBLASTEM:

TECHNICKÉ INFORMACE

- Site
- IP adresy
- Domény a subdomény
- Servery
- Služby a aplikace
- Certifikáty
- MTA konfigurace
- DNS zóny
- Google hacking

LIDSKÉ ZDROJE

- Zaměstnanci
- Emaily
- Hesla
- Identity
- Sociální sítě

DŮLEŽITÉ INFORMACE

- Data leaks
- Darkweb

NAŠE SLUŽBY A ŘEŠENÍ

- Bezpečnostní audity, analýzy a konzultace
- Penetrační testy
- Konfigurační audity
- Pravidelné kontroly *(health checky)*
- Expertní konzultace ochrany před ransomware
- Analýzy shody s ZoKB, ISO 27000 a NÚKIB
- Školení administátorů a uživatelů
- Řešení havarijních situací při kybernetických incidentech

pragodata

PragoData a.s. | Opletalova 1418/23, 110 00, Praha 1 | www.pragodata.com