

Pokročilé metody modelace hrozeb:

Cesta pro zefektivnění bezpečnostních procesů (nejen) státních institucí

Mgr. Ing. Vladimír Mana, LL.M. – MPO

Mgr. Tomáš Poledno – MPO

Ing. Jan Kopřiva – Nettles Consulting



MINISTERSTVO
PRŮMYSLU A OBCHODU



Jak MPO přistupuje ke KB

- ➔ MPO je povinnou osobou dle ZoKB
- ➔ Organizace má zavedený funkční ISMS v souladu s legislativními požadavky
 - ▶ Vybrané aspekty řízení KB legislativa nedefinuje a detailní přístup je nezbytné zvolit dle specifických potřeb organizace
 - ➔ Jednou z oblastí vyžadujících personifikovaný přístup je modelování hrozeb

Proč MPO modeluje kybernetické hrozby?

- ➔ Identifikace hrozeb je nezbytným krokem pro analýzu rizik i identifikaci požadavků na bezpečnostní opatření
- ➔ Katalog hrozeb uvedený ve VoKB je vysoce generický
 - ▶ Pro potřeby konkrétní organizace je sám o sobě principiálně nedostatečný, a navíc omezeně detailní
 - ➔ NÚKIB uvádí, že jde o výchozí/vzorový seznam hrozeb
- ➔ Možnost využití jiných obecně přijímaných oborových standardů
 - ▶ MITRE ATT&CK

K čemu může sloužit MITRE ATT&CK

- ➔ Širší využití než běžný výstup z analýz rizik:
 - ▶ Detailní zacílení detekčních a preventivních bezpečnostních opatření
 - ▶ Možnost specifikace detailních požadavků na bezpečnostní systémy i služby v rámci výběrových řízení



Pokročilé metody modelace hrozeb: Cesta pro zefektivnění bezpečnostních procesů (nejen) státních institucí

Jaké techniky jsou relevantní pro „nás“?

- ➔ Do jisté míry individuální, z významné míry však determinované
 - ▶ Geografickým rozsahem působení organizace
 - ▶ Sektorovým zaměřením organizace
- ➔ Vybrané hrozby (škodliví aktéři, malware,...) jsou relevantní pro všechny, některé hrozby jsou však sektorově či geograficky specifické
 - ▶ Modelování hrozeb s pomocí rámce ATT&CK je založené na identifikaci technik specifických pro ty hrozby, které jsou vysoce relevantní pro naši organizaci

Vytváření modelů hrozeb

DEMO

Výhody modelování hrozeb s pomocí ATT&CK

- ➔ MITRE ATT&CK je široce využívaným de facto standardem v rámci globální bezpečnostní komunity
 - ▶ Mapování útočných kampaní vybraných skupin
 - ▶ Mapování chování škodlivého kódu
 - ▶ Cílení testů bezpečnostních řešení i organizací
 - ▶ Mapování a cílení detekčních mechanismů
- ➔ ATT&CK je standardem v oblasti sdílení dat v KB a pro jakoukoli organizaci řídící KB je proto vhodné jej využívat

Podpora organizací ze strany MPO

- ➔ V rámci MPO bylo původně modelování hrozeb s pomocí ATT&CK prováděno výhradně jako interní aktivita pro posílení KB
- ▶ Detailní modelování hrozeb má však významný přínos pro jakoukoli organizaci v ČR
- ➔ MPO se v souvislosti s tím rozhodlo podpořit nejen zřizované organizace a státní správu, ale i vybrané průmyslové subjekty a české organizace obecně

Cíle plánovaného projektu

- ➔ Vytvoření a periodická aktualizace specifických modelů hrozeb
- ➔ Publikování metodiky pro použití konkrétními sektory a typy organizací:
 - ▶ Ministerstva a jimi zřizované organizace a organizace obdobného charakteru
 - ▶ Organizace z oblasti energetiky a produktovodů
 - ▶ Obecnější modely relevantní adresně pro české organizace a společnosti

Výhody výstupů plánovaného projektu

- ➔ Vysoká znovupoužitelnost vybraných modelů:
 - ▶ Přímé použití pro vybrané oblasti řízení KB v organizacích se základními bezpečnostními potřebami
 - ▶ Pro „vyspělejší“ organizace s komplexnějšími bezpečnostními potřebami mohou pak sloužit jako výchozí bod pro vytváření vlastních, vysoce detailních modelů pro konkrétní prostředí

Závěr

- ➔ V oblasti KB nemá smysl pokoušet se znovu „vymýšlet kolo“
 - ▶ Je vhodné využívat existující standardy a přístupy, ideálně ty s mezinárodním dosahem (NIST, ATT&CK, ...)
- ➔ MPO je specifickou organizací státní správy s přesahem do soukromé sféry, působící na pomezí ČR a mezinárodního světa
 - ▶ Výstupy plánovaného projektu jsme se proto rozhodli využít pro podporu kybernetické bezpečnosti nejen státní správy, ale i vybraných průmyslových subjektů

Děkujeme za pozornost

V případě, že Vás toto téma zaujalo
a měli byste zájem o navázání hlubší
spolupráce, můžete se na nás obrátit
na adrese kb@mpo.gov.cz



MINISTERSTVO
PRŮMYSLU A OBCHODU

