Red Teaming

AEC

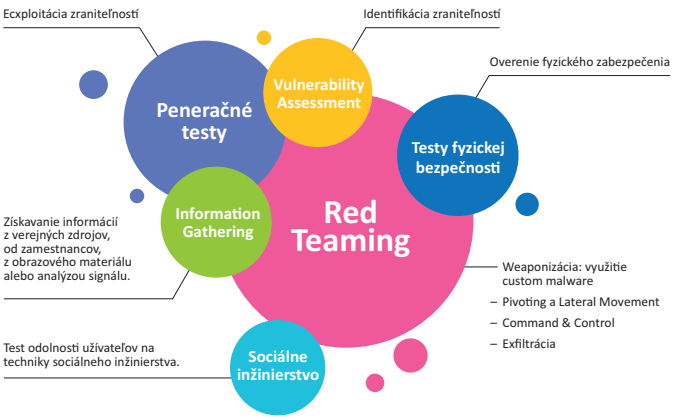
S vývojom nových druhov útokov a s nárastom ich sofistikovanosti, prestáva penetračné testovanie dostatočne plniť svoj účel. Na základe toho je nutné, začať testovať aplikácie a infraštruktúru komplexnejším spôsobom. Štandardné spôsoby testovania odhalia rôzne typy zraniteľností ale nepreveria schopnosť detekcie, reakcie a zotavovania sa z kybernetického útoku.

Služba Red Teaming verne simuluje hrozby útoku s pomocou najmodernejších technológií, taktík a poskytuje informácie o pripravenosti spoločnosti, tieto útoky detegovať, eliminovať a vykonať nápravné opatrenia.

Čo je Red Team?

V rámci kybernetickej bezpečnosti označujeme Red Teamom skupinu skúsených a organizovaných etických hackerov, ktorí majú za úlohu vykonať simulovaný útok na danú entitu. Útok preverí kybernetickú a fyzickú bezpečnosť aj interné procesy a komunikáciu v rámci technických a ďalších tímov, ktoré majú na starosť kybernetickú bezpečnosť. Celé cvičenie sa uskutočňuje ako utajená operácia, o ktorej je informovaná iba veľmi malá skupina ľudí – spravidla najvyššie vedenie spoločnosti.

Red Team verne simuluje taktiky, techniky a postupy reálnych útočníkov. Vhodnou definíciou cieľov overujeme efektívnosť ľudí, procesov a technológií použitých k obrane spoločnosti. V rámci Red teaming cvičení budú Vaši zamestnanci nepriamo školený reálnymi situáciami v kontrolovanom režime, bez hrozby reálnych škôd.



www.aec.sk

Red Teaming

Definícia rolí

RED TEAM
Naši špecialisti, ktorí simulujú taktiku, techniky a postupy útočníkov.

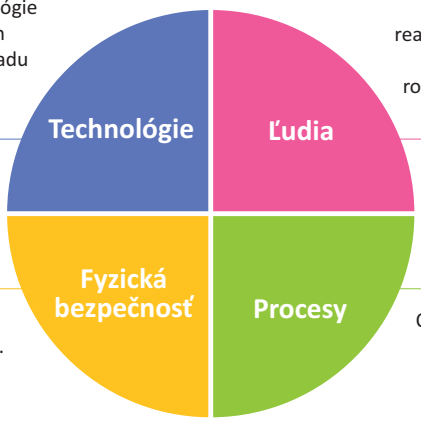
WHITE TEAM
Vybraný tím z manažmentu spoločnosti, ktorý dohliada na prebiehajúce cvičenia.

BLUE TEAM
Tím interných security špecialistov spoločnosti, ktorí detegujú útok a vykonávajú nutné protiopatrenia.

Red Teaming

Red Team preverí technológie nielen z pohľadu možných zraniteľností ale aj z pohľadu účinnosti nasadených obranných nástrojov.

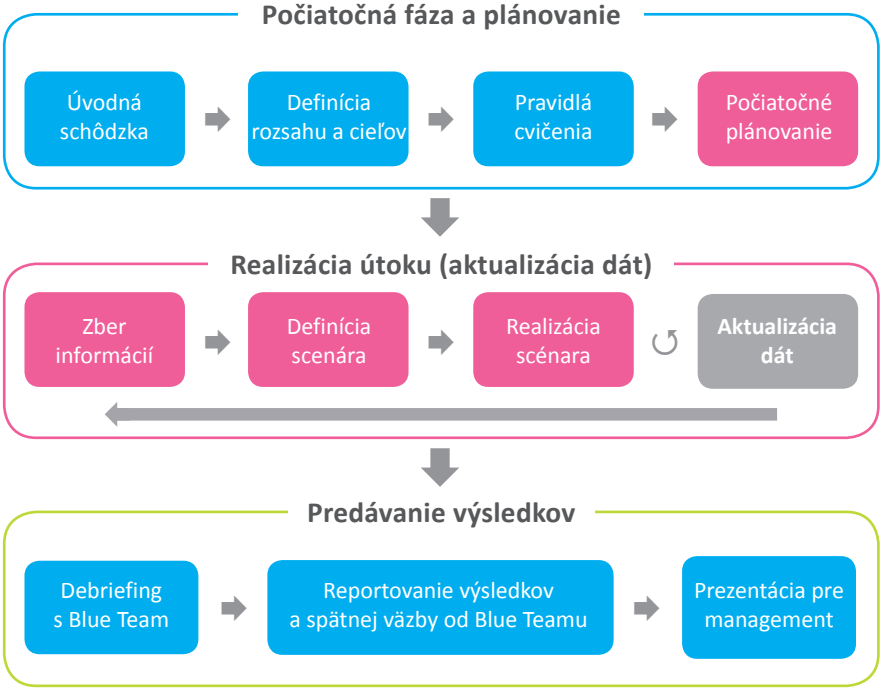
Preverí schopnosť ľudí reagovať v prípade reálneho útoku a uskutočneného rozhodnutia managementu v krízovej situácii.



Otestuje fyzické zabezpečenie organizácie.

Overí nastavenie procesov vnútri spoločnosti.

Priebeh projektu



– potrebná súčinnosť – bez súčinnosti

Testovanie delíme do štyroch skupín:

Technológie
Interná infraštruktúra, cloud, aplikácie (webové, mobilné), servery, koncové zariadenia atď..

Ľudia
Interný a externý personál (zamestnanci, kontraktori, dodávatelia, obchodní partneri atď..).

Procesy
Interné procesy (existencie, formálnosť, ucelenosť a dodržiavanie), komunikácia medzi členmi obranného tímu.

Fyzická bezpečnosť
Testovanie fyzickej bezpečnosti budov, skladísk, datacentier, výrobných závodov atď..

Vykonávame penetračné testy, potrebujeme Red Teaming?

Penetračné testovanie a vulnerability scanning sú neoddeliteľnou súčasťou bezpečnosti a je nutné tieto aktivity zachovať, dodržiavať a rozvíjať. Avšak takýto metodický prístup nie je schopný otestovať reálnu pripravenosť a tým čeliť kybernetickým hrozbám. Red Teaming, ako simulácia reálneho útoku, skutočne overí pripravenosť a schopnosť reakcie.

Penetračné testy
- Krátka doba trvania (1–3 týždne)
- Administrátori a vlastníci aplikácie vedia o prebiehajúcom testovaní
- Mieri na nájdenie zraniteľností v danej aplikácii či infraštruktúre
- Striktne definovaný obmedzený rozsah
- Dodatočné vrstvy ochrany (WAF, IPS, atď.) môžu byť na tento účel testov deaktivované
- Často realizovaný v neprodukčnom prostredí

Red Teaming
- Dlhšia doba trvania (priemerne 1–3 mesiace)
- Utajený priebeh, iba členovia White Teamu vedia o aktivite
- Neobmedzené testovanie všetkých vrstiev ochrany ako celku (technológie, ľudia, procesy, fyzická bezpečnosť)

AEC s. r. o., Prievozská 6, 821 09 Bratislava, tel.: +421 254 410 283
AEC a.s., Voctářova 20a, 180 00 Praha 8, tel: +420 226 229 133
AEC a.s., Veveří 102, 616 00 Brno, tel: +420 541 235 466

www.aec.sk