Red Teaming

AEC

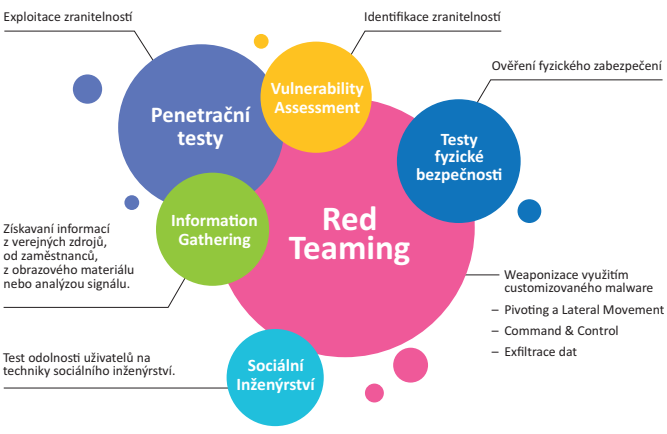
S vývojem nových druhů útoků, a s nárůstem jejich sofistikovanosti, přestává penetrační testování dostatečně plnit svůj účel. Proto je nutné začít testovat aplikace a infrastrukturu komplexnějším způsobem. Standardní způsoby testovaní odhalí různé typy zranitelností, ale neprověří schopnost detekce, reakce a zotavení z kybernetického útoku.

Služba Red Teaming věrně simuluje hrozby útoků s pomocí nejmodernějších technologii, taktik a poskytuje informace o připravenosti společnosti tyto útoky detekovat, eliminovat a provést nápravná opatření.

Co je Red Team?

V rámci kybernetické bezpečnosti označujeme Red Teamem skupinu zkušených a organizovaných etických hackerů, kteří mají za úkol provést simulovaný útok na danou entitu. Útok prověří kybernetickou a fyzickou bezpečnost i interní procesy a komunikaci v rámci technických a dalších týmů, které mají na starost kybernetickou bezpečnost. Celé cvičení se provádí jako utajená operace, o které je informována pouze velmi úzká skupina lidí – zpravidla nejvyšší vedení společnosti.

Red Team věrně simuluje taktiky, techniky a postupy reálných útočníků. Vhodnou definicí cílů ověřujeme efektivnost lidí, procesů a technologií použitých k obraně společnosti. V rámci Red teaming cvičení budou vaši zaměstnanci nepřímo školeni reálnými situacemi v kontrolovaném režimu, bez hrozby reálných škod.



www.aec.cz

Red Teaming

Definice rolí

RED TEAM
Naši specialisté, kteří simulují taktiku, techniky a postupy útočníků.

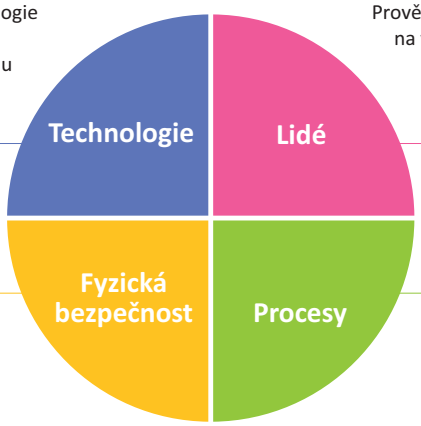
WHITE TEAM
Vybraný tým z managementu společnosti, který dohlíží na probíhající cvičení.

BLUE TEAM
Tým interních security specialistů společnosti, který detekuje útok a provádí nutná protiopatření.

Red Teaming

Red Team prověří technologie nejen z pohledu možných zranitelností, ale z pohledu účinnosti nasazených obranných nástrojů.

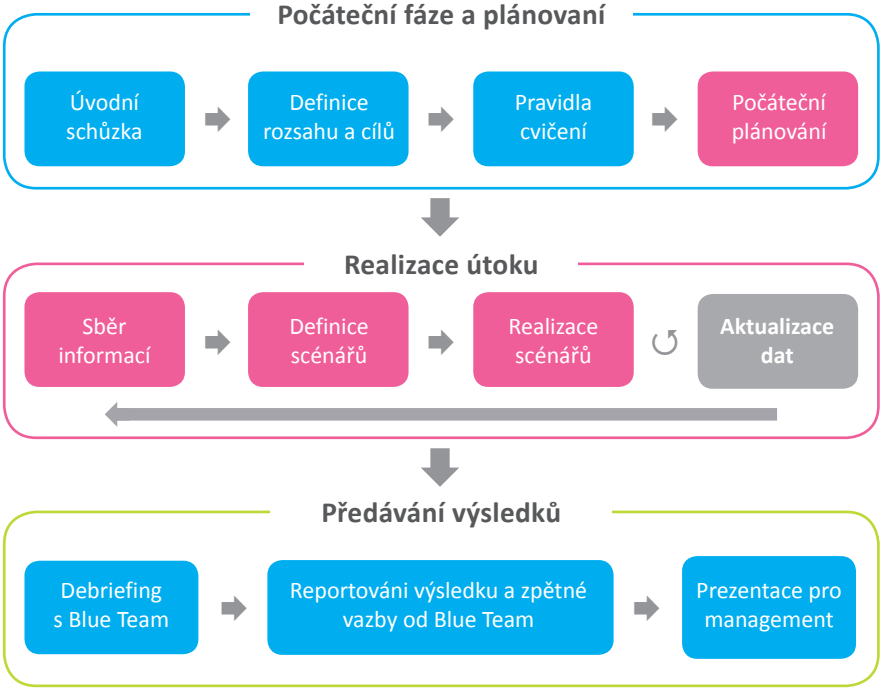
Prověří schopnost lidí reagovat na v případě reálného útoku a učiněné rozhodnutí managementu v krizové situaci.



Otestuje fyzické zabezpečení organizace.

Ověří nastavení procesů uvnitř společnosti.

Průběh Red Teaming projektu



– nutná součinnost – bez součinnosti

Testování dělíme do čtyř skupin:

Technologie
Interní infrastruktura, cloud, aplikace (webové, mobilní), servery, koncová zařízení atd.

Lidé
Interní a externí personál (zaměstnanci, kontraktoři, dodavatelé, obchodní partneři atd.).

Procesy
Interní procesy (existence, formálnost, ucelenost a dodržování), komunikace mezi členy obranného týmu.

Fyzická bezpečnost
Testování fyzické bezpečnosti budov, skladišť, datacenter, výrobních závodů atd.

Potřebuji Red Teaming při penetračních testech?

Penetrační testovaní a vulnerability scanning jsou nedílnou součástí bezpečnosti a je nutné tyto aktivity zachovat, dodržovat a rozvíjet. Avšak takový metodický přístup není schopen otestovat reálnou připravenost a tím čelit kybernetickým hrozbám. Red Teaming, jako simulace reálného útoku, skutečně ověří připravenost, schopnost reakce i následného zotavení.

Penetrační testy
- Krátká doba trvání (1–3 týdny)
- Administrátoři a vlastníci aplikace vědí o probíhajícím testování
- Cílí na nalezení zranitelností v dané aplikaci či infrastruktuře
- Striktně definovaný omezený rozsah
- Dodatečné vrstvy ochrany (WAF, IPS, atp) mohou být pro účel testů deaktivovány
- Často realizovány na neprodukčním prostředí

Red Teaming
- Delší doba trvání (průměrně 1–3 měsíce)
- Utajený průběh, pouze členové White Teamu vědí o aktivitě
- Neomezené testování všech vrstev ochrany jako celku (technologie, lidé, procesy, fyzická bezpečnost)
- Zasahuje produkčním prostředí

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
AEC s. r. o., Prievozská 6, 821 09 Bratislava, tel.: +421 254 410 283