Dokument je optimalizován pro Adobe Reader. Nezaručujeme správné zobrazení v jiných prohlížečích.

Red Teaming

AEC

security is our DNA

Red Teaming

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 postupy testovaní sice odhalí různé typy zranitelností, ale neprověří schopnost detekce, reakce ani zotavení z kybernetického útoku.

Stejně jako se vyvíjejí nové technologie, zdokonalují se i metody a taktiky útočníků. Společnosti se tak musí adaptovat, aby lépe chránily svá aktiva i klienty. Musí být schopny nejen reaktivního přístupu ke kybernetickým hrozbám, ale je třeba, aby začaly hrozby také proaktivně vyhledávat, a tím eliminovaly možné finanční, reputační a jiné dopady.

Služba Red Teaming věrně simuluje hrozby útoků s pomocí nejmodernějších technologií a taktik, a díky tomu dokáže klientovi poskytnout informace o tom, jak je jeho společnost připravena tyto útoky detekovat, eliminovat a provést nápravná opatření.

Red Team

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

Red Teaming představuje věrnou simulaci komplexních a sofistikovaných kybernetických útoků. Napadeným, tedy Blue Teamu, umožňuje připravit se na reálné hrozby a v případě potřeby smysluplně zareagovat, tj. přejít z reaktivního na proaktivní myšlení. Díky dobře osvojeným postupům lze po útoku pohotově provádět nezbytné úkony k obnovení provozu.

AEC

security is our DNA

Red Teaming

Weaponizace s pomocí malwaru na míru, atd.

Pivoting a Lateral Movement

Command & Control

Exfiltrace dat

Penetrační testy

Exploitace zranitelností

Vulnerability Assessment

Identifikace zranitelností

Sociální inženýrství

Test odolnosti uživatelů pomocí technik sociálního inženýrství.

Information Gathering

Získavaní informací z veřejných zdrojů,od zaměstnanců, z obrazového materiálu nebo analýzou signálu.

Testy fyzické bezpečnosti

Ověření fyzického zabezpečení

Definice rolí

Red Team	White Team	Blue Team
Naši specialisté, kteří simulují taktiky, techniky a postupy útočníků.	Vybraný tým z managementu společnosti, který dohlíží na probíhající cvičení.	Tým interních security specialistů společnosti, který detekuje útok a provádí nutná protiopatření.

Technologie

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

Lidé

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

Fyzická bezpečnost

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

Procesy

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

Red Teaming

Technologie

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

Lidé

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

Fyzická bezpečnost

Prověří fyzické zabezpečení organizace.

Procesy

Prověří nastavení procesů uvnitř společnosti. Schopnost lidí reagovat na reálný útok a účinost krizového řízení.

AEC

security is our DNA

Cíle cvičení

Red Teaming umožní vaší organizaci držet krok nejen s pokročilými technikami kybernetických hrozeb, ale také s útoky vedenými metodami sociálního inženýrství či fyzickou bezpečností. V rámci cvičení vycházíme z ověřených metodik, které věrně simulují reálné útočné metody a taktiky:

MITRE ATT&CK

Cyber Kill Chain

Unified Kill Chain

Advanced Persistent Thread (APT)

Sofistikované techniky zaměřené na konkrétní cíle.

Všechna cvičení podrobně definujeme a provádíme na základě konkrétních požadavků klientů. Díky tomu dokážeme velice přesně pokrýt veškeré klíčové potřeby testovaných organizací. Red Teamingem zmapujeme jak čas nutný k detekci (Mean Time to Detect - MTTD), tak i samotnou reakci na útok (Mean Time to Resolve - MTTR). Ze zjištěných hodnot jsme schopni vyvodit, jak dlouho trvá Blue Teamu detekovat hrozbu, a zanalyzujeme, jakým způsobem se pokouší zmírnit její dopad a provést nápravná opatření.

Mitre attack: https://attack.mitre.org/
Cyber Kill Chain: https://www.csacademy.nl/images/scripties/2018/Paul-Pols---The-Unified-Kill-Chain.pdf
APT groups: https://www.fireeye.com/current-threats/apt-groups.html
Unified Kill Chain: https://www.csacademy.nl/images/scripties/2018/Paul_Pols_-_The_Unified_Kill_Chain_1.pdf

Pro koho je služba určena

Často slýcháme, že některá společnost je příliš malá na Red Teamingová cvičení. Útočníci však dnes cílí na společnosti všech velikostí. Neusilují jen o vaše data. Zaměřují se také na technologie, které následně zařadí do svého botnetu, aby lépe skryli svoje aktivity.

V AEC dokážeme Red Teaming přizpůsobit vaší společnosti na míru. Zohledníme přitom veškeré klíčové aspekty, jako jsou velikost firmy a odvětví, v němž se pohybuje. Zároveň neopomeneme na případná specifika, díky nimž se vaše společnost odlišuje od jiných.

Motivace

S vývojem nových technologií se rozšiřují možnosti jejich využití. Přibývá stále důmyslněji vedených útoků, cílených jak na podpůrnou infrastrukturu, tak na samotné zaměstnance. Red Teaming otestuje, zda vaše kybernetické a fyzické zabezpečení odpovídá doporučeným standardům, a zároveň ověří, do jaké míry panuje soulad mezi reakcí zaměstnanců na probíhající incident a nastavením vnitřích směrnic a procesů.

Dalším nezanedbatelným přínosem cvičení je, pomoc s identifikací a zlepšení klasifikace klířových aktiv a s tím související úroveň ochrany. To může vést – především v souvislosti s nařízením GDPR, resp. ochranou osobních údajů – k významnému snížení rizika úniku dat a následnými finančními sakcemi.

Penetrační testy vs. Red Teaming

AEC

security is our DNA

Penetrační testovaní a skenování zranitelností jsou nedílnou součástí aktuálních bezpečnostních standardů. Tyto aktivity je nezbytné zachovat, dodržovat a dále rozvíjet. Přesto je třeba mít na paměti, že se jedná o čistě metodický přístup, který není schopen otestovat reálnou připravenost a pomoci Vám čelit pokročilým kybernetickým hrozbám.

Vaši připravenost a schopnost reakce na současné typy hrozeb ověří jen dokonalá simulace reálného útoku v podobě Red Teamingu.

Penetrační testy

- Krátká doba trvání (1–3 týdny)
- Administrátoři a vlastníci aplikace/ infrastruktury vědí o probíhajícím testování
- Cílí na nalezení zranitelností vůči konkrétní 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, o aktivitě vědí pouze členové White Teamu
- Neomezené testování všech vrstev ochrany jako celku (technologie, lidé, procesy, fyzická bezpečnost)
- Ověření produkčního prostředí

Komplexnost testování

	Testy sociálním inženýrstvím	Penetrační testy	Red Teaming
Tajný, neohlášený	●	×	●
Neomezený rozsah	×	×	●
Flexibilní přístup	●	×	●
Testování aplikací	×	●	●
Testování on-premise infrastruktury	×	●	●
Testování off-premise infrastruktury	×	●	●
Phising, Vishing	●	×	●
Vytváření malwaru na míru	×	×	●
Fyzická infiltrace	●	×	●
Incident Response Management	×	×	●

Porovnání dle funkcí Risk Managementu

Vulnerability Assessment

Penetrační testování

Red Teaming

Identifikace
Ochrana

Detekce

Reakce
Zotavení

AEC

security is our DNA

Průběh Red Teaming projektu

Počáteční fáze a plánovaní → Realizace útoku → Předání výsledků

Úvodní schůzka
- Počáteční analýza

Definice rozsahu a cílů
- Vymezení cílů, např. infiltrace budovy, kompromitace serverů, zcizení citlivých e-mailů atp.

Pravidla cvičení
- Stanovení pravidel cvičení, povolené a zakázané aktivity, časování, komunikační a eskalační matice

Počáteční plánování
- Příprava a plánování aktivit

Sběr informací
- OSINT, HUMINT, IMINT, SIGINT
- Skenování infrastruktury
- Skenování aplikací
- Dumpster diving
- Google dorking

Definice scénářů
- V závislosti na získaných informacích se definují vektory útoků
- Metodiky MITRE ATT&CK, Cyber Kill Chain, Unified Kill Chain

Realizace scénářů
- Provádění útoku za účelem dosažení definovaných cílů
- Detailní záznam všech prováděných aktivit v časové ose

↺

Aktualizace dat

Debriefing s Blue Teamem
- Technická schůzka se členy obranného týmu
- Detailní rozbor útočných aktivit a následných reakcí Blue Teamu

Report a zpětná vazba od Blue Team
- Finalizace závěrečného reportu
- Detailní časová osa útočných aktiv v korelaci s činností obránců

Prezentace pro management
- Prezentace zjištěných nedostatků
- Doporučení nápravných opatření

■ – nutná součinnost ■ – bez součinnosti

OSINT – Open-Source INTelligence

Získávání informací z veřejných zdrojů. Dostupné informace z internetu, DNS, certifikátů, veřejných služeb atd.

HUMINT – Human Intelligence

Získávání informací s využitím sociálního inženýrství. Telefonáty, e-maily, dotazníky, shoulder surfing, Insider Threat apod.

IMINT – Imaginery Intelligence

Získávání informací z obrazového materiálu.

Snímky z obrazovky, lístečky na PC atd.

SIGINT – Signals Intelligence

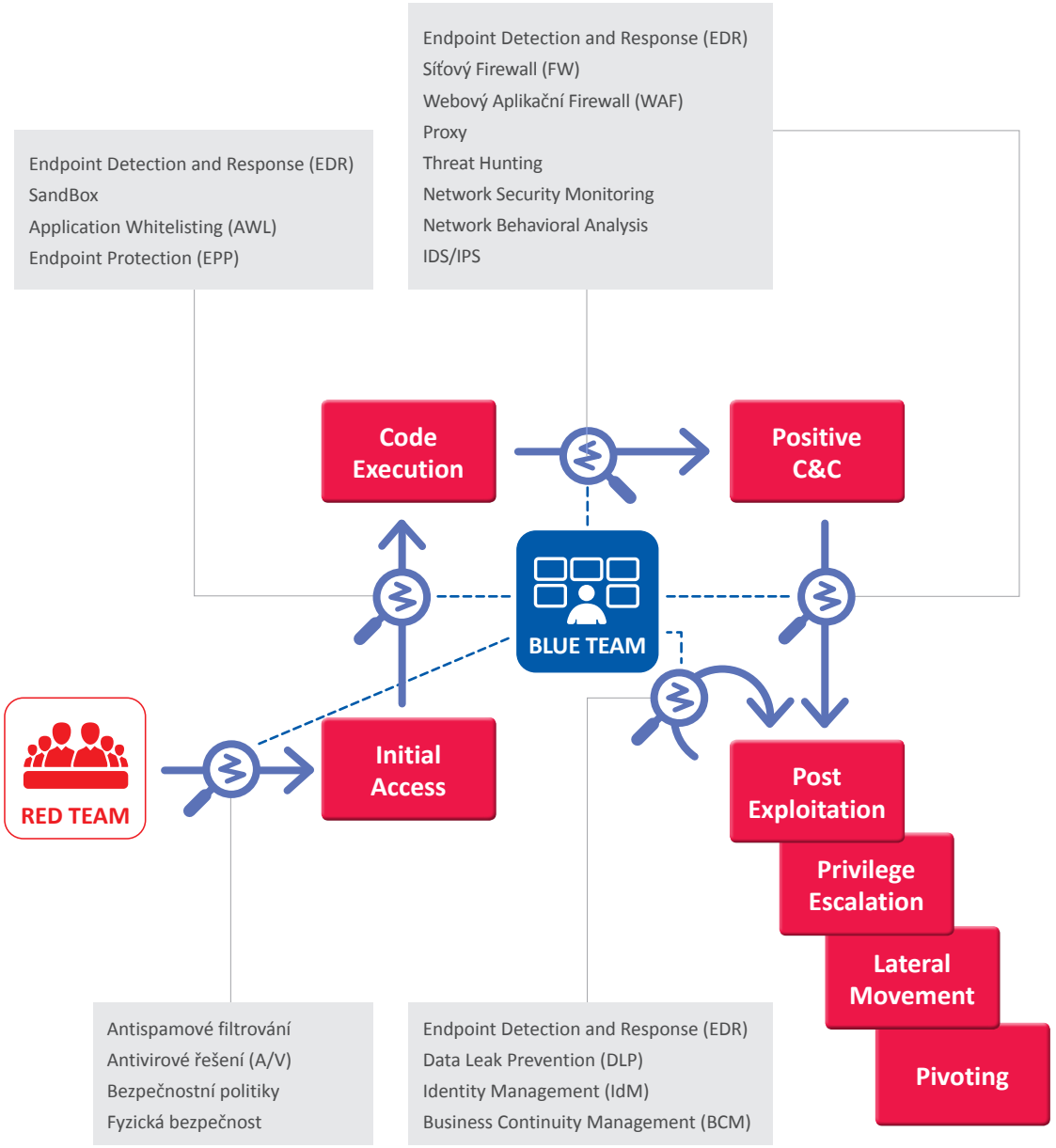
Získávání informací analýzou signálů.

Wiretapping, Rouge AP, připojení rozbočovače do sítě atd.

AEC

security is our DNA

Red Team Assessment – technická fáze



AEC

security is our DNA

Struktura scaningu

Kybernetická bezpečnost

- Interní infrastruktura
- Externí infrastruktura
- Cloud
- Wifi
- Webové aplikace
- Tiskárny
- Výtahy
- IoT
- TV
- CCTV
- IP telefony

AEC

security is our DNA

Struktura scaningu

Fyzická bezpečnost

- Odposlechy
- Čipové karty
- Media drop
- Fyzický průnik do objektu
- Zajištění/prověření obrany perimetru
- Neautorizovaná zařízeni ve vnitřní síti
- Dumpster diving
- Společné prostory
- Zcizení HW
- Chytrý telefon

AEC

security is our DNA

Struktura scaningu

Procesní bezpečnost

- Vyhodnocení interních procesů
- Interní zpráva o komunikaci týmů
- Incident Response
- Impersonace
- Tailgating

Výsledný report

- Analýzu současného stavu zabezpečení vaší společnosti, včetně detailního výpisu všech aktivit umožňujících překonání stávajících obranných mechanismů.
- Dosažení vytyčených cílů a nutných kroků vedoucích k eliminaci daných vektorů útoků.
- Detailní popis scénářů (taktik, technologií a procesů) použitých ke kompromitaci prostředí a dosažení definovaných cílů.
- Detailní seznam provedených aktivit, tzv. logbook.

AEC

security is our DNA

Příklad průběhu projektu

1

3 týdny

- Úvodní schůzka
- Definice cílů a pravidla cvičení
- Příprava scénářů útoků

2

2 měsíce

- DoS attack (odvedení pozornosti)
- Spear Phising
- Web server attack
- Infekce uživatelské stanice malwarem
- Infekce web serveru malwarem
- DoS mitigace Blue team
- Eskalace privilegií
- Zřízení persistentního přístupu
- Lateral movement
- AD hive dump
- Password cracking
- Splnění cílů

3

1–2 týdny

- Debriefing s Blue teamem
- Vytváření finální zprávy
- Prezentace pro management

AEC

security is our DNA

Proč si vybrat AEC

Náš Red Teaming vychází z metodik Unified Kill Chain, Cyber Kill Chain, MITRE ATT&CK a APT technik, ale především těží z našich mnohaletých zkušeností. V týmu máme odborníky z unikátního Cyber Defense Centra (náš Blue Team) a další specialisty s praxí v následujících oblastech:

- **penetrační testování** – webové aplikace, interní a externí infrastruktura, mobilní zařízení a IoT
- **sociální inženýrství** – v prostorách společnosti, e-mailové a telefonické phisingové kampaně
- **fyzická bezpečnost** – otevírání zámků, obcházení kamerových systémů a obcházení alarmů

Průběžné informování o stavu projektu a aktivitách je pro nás samozřejmostí. V případě nalezení kritické zranitelnosti okamžitě navrhneme nutná protiopatření. Kompletní výstupy Vám následně poskytneme v detailní závěrečné zprávě formou workshopů.

30 let zkušeností

> 20 špičkových etických hackerů

> 1000 projektů během 3 let

vlastní vývoj testovacích nástrojů

prověření NBÚ na stupeň důvěrné

AEC security is our DNA

www.aec.cz