Penetračné testy

Preverte úroveň zabezpečenia svojich systémov a aplikácií skôr, než to urobí niekto cudzí.

AEC

Robíme simulácie kybernetických útokov na systémy, aplikácie aj celú infraštruktúru. Z našej ponuky si môžete vybrať špecifické penetračné testy pre konkrétne aplikácie a systémy. S Red Teaming cvičeniami overíte schopnosť detekcie útoku a správnej reakcie prostredníctvom vašich procesov a bezpečnostných špecialistov. Ponúkame aj službu simulujúcu phishingové útoky s využitím metód sociálneho inžinierstva.

Naším cieľom je odhaliť hrozby a zraniteľnosti, ktoré môžu narušiť dôvernosť, integritu či dostupnosť vašich systémov a aplikácií. Výstupom našej práce je záverečná správa, ktorá obsahuje nájdené zraniteľnosti s opisom, ako ich replikovať, závažnosť možných rizík a odporučení na odstránenie nájdených chýb. Na záverečnom workshope oboznámime váš tím s priebehom testov a detailne rozoberieme jednotlivé nálezy, prípadne je možné spoluprácu rozšíriť o nadväzujúce školenia na danú problematiku.

www.aec.sk

Ponúkame služby

- **Penetračné testy aplikácií**
  - Webové
  - Mobilné
  - Desktopové
  - API
- **Penetračné testy infraštruktúry**
  - Interné
  - Externé
  - Záťažové testy/DoS
  - Wi-Fi siete
  - Riadiace systémy/ICS
  - VoIP
  - IoT
- **Konfiguračné testy**
  - Operačné systémy
  - Cloud
- **Špecializované testy a služby**
  - ATM
  - RFID
  - Reverse Engineering
  - Phishing
  - Ransomware
  - Revízia zdrojového kódu
- **Testy sociálnym inžinierstvom**
- **Red Teaming**

Penetračné testy aplikácií

Webové
Pri testovaní aplikácií je naším cieľom odhalenie zraniteľností, ktoré môžu narušiť ich dôvernosť, integritu či dostupnosť. V rámci aplikačnej bezpečnosti sa zaoberáme nielen bežnými útokmi zneužívajúcimi typické zraniteľnosti, ale venujeme sa tiež návrhu či architektúre danej aplikácie.

Mobilné
Pri testoch mobilných aplikácií hľadáme chyby v ich implementácii aj v samotných zariadeniach. Pri aplikáciách analyzujeme možné rizika a hľadáme bezpečné riešenia pre používanie mobilných zariadení vo firemnom prostredí. Pri mobilných telefónoch robíme forenznú analýzu prístrojov, ktoré sa stali terčom hackerských útokov. S využitím týchto skúseností pomáhame s tvorbou bezpečných aplikácií.

Desktopové
Pri desktopových aplikáciách postupujeme pomocou dekompilácie až na úroveň zdrojového kódu vrátane jeho úprav. Identifikujeme z pohľadu bezpečnosti rizikové miesta, citlivé dáta alebo iné nedostatky v autorizácii či samotnom prenose medzi klientskou aplikáciou a serverom.

API
API penetračnými testami preverujeme slabiny rozhrania pre poskytovanie služieb. Pri API testujeme rôzne typy rozhraní, medzi ktoré najčastejšie patrí REST a SOAP. Pri testovaní využívame relevantné časti metodiky OWASP pre testovanie webových aplikácií a tiež našu vlastnú metodiku, ktorá sa vyvinula z našich skúseností testovaním API služieb, PSD2 a iných.

Konfiguračné testy

Operačné systémy
Pri operačných systémoch preverujeme mieru zabezpečenia jednotlivých konfiguračných prvkov. Ponúkame aj implementáciu odporučení, ktoré vám na základe výsledkov z nami vykonaných testov vystavíme, eliminujeme tak nájdené slabiny a zvyšujeme obranyschopnosť pri nečakanom reálnom útoku.

Cloud
Migrácia firemnej infraštruktúry do cloudového prostredia sa stáva trendom. Kľúčovú rolu predstavuje konfigurácia cloudových služieb, či už natívnych, alebo služieb tretích strán. Konfiguračné nedostatky môžu viesť k strate firemných dát aj dôvery zákazníkov, preto sme pripravení vám s otázkou bezpečnej konfigurácie vášho cloudového prostredia pomôcť.

Testy sociálnym inžinierstvom

Sociálne inžinierstvo je akt, v ktorom sa sociálny inžinier pokúša prinútiť svoj cieľ k vykonaniu akcie, ktorá nemusí byť v najlepšom záujme daného subjektu. Zamestnanci sú považovaní za najslabší článok bezpečnosti v spoločnosti. Útočník tak môže využiť sociálne inžinierstvo na prelomenie aj tých najzabezpečenejších perimetrov. Sociálni inžinieri na to využívajú útoky ako napríklad vishing, phishing alebo fyzickú infiltráciu pomocou impersonácie. Naším cieľom je preveriť zabezpečenie vašej spoločnosti za pomoci týchto metód a následne navrhnúť najlepšie riešenie pre elimináciu nájdených rizík.

Penetračné testy infraštruktúry

Interné
Pri penetračných testoch internej infraštruktúry mapujeme vnútornú sieť spoločnosti, identifikujeme aktívne sieťové prvky a preverujeme ich bezpečnosť. Pokúšame sa prelomiť vybrané systémy a kompromitovať doménu spoločnosti eskaláciou privilégií z bežného používateľa na doménového administrátora. Súčasťou sú tiež testy z pracovnej stanice bežného používateľa.

Externé
Pri penetračných testoch externej infraštruktúry kladieme dôraz na odhalenie všetkých dostupných sieťových služieb, komponentov a ich detailnú enumeráciu. Zber verejných informácií o sieťovej infraštruktúre spoločnosti je pre útočníka kľúčový. Na tento účel využívame tak automatizované, ako aj vlastné proprietárne nástroje a metodiky.

Záťažové
Útočníci často pri kľúčových webových aplikáciách poškodzujú weby spoločností tým, že ich jednoducho znepristupnia. Čím dlhšie nie je používateľom daná webová aplikácia dostupná, tým väčšie sú straty. V rámci Denial of Service testujeme vybrané služby, aby k týmto situáciám nedochádzalo a kritické webové aplikácie tak fungovali aj pri neočakávane vysokej záťaži.

Wifi siete
Penetračnými testami Wi-Fi technológií simulujeme útok na prístup do vnútornej siete organizácie prostredníctvom bezdrôtového signálu Wi-Fi sietí. Po získaní prístupu preveríme kvalitu filtrovania prevádzky medzi sieťovým segmentom Wi-Fi klientov a zvyškom interných sietí. Do testov zahŕňame aj analýzy konfigurácie pripojenia k bezdrôtovej sieti na strane klientskych zariadení.

SCADA
Zaistíme, aby boli vaše riadiace systémy (SCADA) zabezpečené pred vonkajšími aj vnútornými hrozbami za pomoci penetračných testov. SCADA systémy sú veľmi často zastarané a plné zraniteľností, ľahko sa tak stávajú terčom APT útokov. Mnoho systémov nie je aktualizovaných, zo strachu z nefunkčnosti či zastavenia výroby, tieto nedostatky môžu útočníci ľahko zneužiť na ich ovládnutie.

VoIP
Zaisťujeme penetračné testy na verejne dostupnú kritickú infraštruktúru organizácie, ako sú telefónne systémy VoIP. Pomocou metódy man-in-the-middle odpočúvajú útočníci komunikáciu medzi prichádzajúcim a odchádzajúcim pripojením telefónov. Môžu tak získať prístup k chúlostivým dátam v internej sieti VoIP. Preveríme všetky slabé miesta, aby vo vašej organizácii k takým situáciám nedochádzalo.

IoT
Naším hlavným zameraním pri testovaní internetu vecí (IoT) je zistenie, akým jednoduchým cieľom dané zariadenia sú. Aké informácie z nich možno získať a ako detegovať ich zraniteľnosti, ktoré môžu byť zneužité na získanie neautorizovaných prístupov či krádeží dát.

Špecializované testy a služby

ATM

Preveríme zraniteľnosti bankomatov v priebehu jedného týždňa. Naša komplexná analýza zah=rňa spôsoby fyzického prístupu, eskaláciu privilégií, testy operačného systému a aplikácií. Môžeme sa však sústrediť iba na penetračné testy infraštruktúry, integračných služieb a manažmentu, reverznú analýzu softvéru, prípadne bezpečnostnú analýzu zdrojového kódu.

RFID

Pri RFID technológiách replikujeme verejne známe útoky na konkrétne typy kariet a takisto sa púšťame do vlastného prieskumu možných slabých miest a potenciálnych vektorov útoku.

Reverse Engineering

Pri reverznom inžinierstve spätne analyzujeme funkčnosti testovaných aplikácií, bez prístupu či znalosti ich zdrojových kódov, a tým overíme ich odolnosť proti možným reálnym útokom. Pri analýze kódov využívame skúsenosti z penetračných testov desktopových klientov.

Phishing

Testujeme odolnosti firiem proti útokom vydieračskými programami. Pri preverovaní analyzujeme súčasné situácie vrátane testu odolnosti systému. Výstupom je report s odporučeniami príslušných riešení.

Ransomware

Ponúkame unikátnu službu na test odolnosti vašej organizácie voči ransomware. Dokáže vaša bezpečnostná technológia či mechanizmy odhaliť tento typ malwaru? Sú vaši zamestnanci dostatočne preškolení, aby ransomware nespustili vo vašej sieti? To všetko vám povieme.

Codebashing

Ak vyvíjate aplikácie, ponúkame vám prostredníctvom služby Codabashing riešenie pre edukáciu a evangelizáciu v oblasti aplikačnej bezpečnosti. Tá umožňuje bezpečnostným a vývojovým tímom vytvárať a udržiavať kultúru bezpečného vývoja. Prostredníctvom komunikačných nástrojov, gamifikácie, vzájomných výziev a priebežných hodnotení vám Codebashing pomôže eliminovať vznik softvérových zraniteľností v zdrojovom kóde.

Red Teaming

S Red Teamingem ideme ďaleko za hranice klasických penetračných testov tým, že verne simulujeme útoky reálnych hackerských skupín a snažíme sa overiť komplexné zabezpečenie organizácie nielen v technologickej oblasti, ale aj na úrovni interných procesov a interných bezpečnostných špecialistov. Na rozdiel od penetračných testov, keď sa od zadávateľa bežne vyžaduje určitá miera súčinnosti, robíme Red Teaming ako blackbox – všetky informácie o cieli zisťujeme až v priebehu akcie a snažíme sa zostať v utajení čo najdlhšie.