Penetrační testy

Prověřte úroveň zabezpečení svých systémů a aplikací dříve, než to udělá někdo cizí.

Provádíme simulace kybernetických útoků na systémy, aplikace i celou infrastrukturu. Z naší nabídky si můžete vybrat specifické penetrační testy pro konkrétní aplikace a systémy. S Red Teaming cvičeními ověříte schopnost detekce útoku a správné reakce prostřednictvím vašich procesů a bezpečnostních specialistů. Nabízíme i službu simulující phishingové útoky s využitím metod sociálního inženýrství.

Naším cílem je odhalit hrozby a zranitelnosti, které mohou narušit důvěrnost, integritu či dostupnost vašich systémů a aplikací. Výstupem naší práce je závěrečná zpráva, která obsahuje nalezené zranitelnosti s popisem, jak je replikovat, závažnost možných rizik a doporučení k odstranění nalezených chyb. Na závěrečném workshopu seznámíme váš tým s průběhem testů a detailně rozebereme jednotlivé nálezy, případně je možné spolupráci rozšířit o navazující školení na danou problematiku.

www.aec.cz

AEC

Nabízíme služby

- **Penetrační testy aplikací**
  - Webové
  - Mobilní
  - Desktopové
  - API
- **Penetrační testy infrastruktury**
  - Interní
  - Externí
  - Zátěžové testy/DoS
  - Wi-Fi sítě
  - Řídící systémy/ICS
  - VoIP
  - IoT
- **Konfigurační testy**
  - Operační systémy
  - Cloud
- **Specializované testy a služby**
  - ATM
  - RFID
  - Reverse Engineering
  - Phishing
  - Ransomware
  - Revize zdrojového kódu
- **Testy sociálním inženýrstvím**
- **Red Teaming**

Penetrační testy aplikací

Webové
Při testování aplikací je naším cílem odhalení zranitelností, které mohou narušit jejich důvěrnost, integritu či dostupnost. V rámci aplikační bezpečnosti se zabýváme nejen běžnými útoky zneužívajícími typické zranitelnosti, ale věnujeme se také návrhu či architektuře dané aplikace.

Mobilní
Při testech mobilních aplikací hledáme chyby v jejich implementaci i v samotných zařízeních. U aplikací analyzujeme možná rizika a hledáme bezpečná řešení pro užívání mobilních zařízení ve firemním prostředí. U mobilních telefonů provádíme forenzní analýzu přístrojů, které se staly terčem hackerských útoků. S využitím těchto zkušeností pomáháme s tvorbou bezpečných aplikací.

Desktopové
U desktopových aplikací postupujeme pomocí dekompilace až na úroveň zdrojového kódu, včetně jeho úprav. Identifikujeme z pohledu bezpečnosti riziková místa, citlivá data nebo jiné nedostatky v autorizaci či samotném přenosu mezi klientskou aplikací a serverem.

API
API penetračními testy prověřujeme slabiny rozhraní pro poskytování služeb. U API testujeme různé typy rozhraní, mezi které nejčastěji patří REST a SOAP. Při testování využíváme relevantní části metodiky OWASP pro testování webových aplikací a také naší vlastní metodiku, která vzešla s našich zkušeností testováním API služeb, PSD2 a jiných.

Konfigurační testy

Operační systémy
U operačních systémů prověřujeme míru zabezpečení jednotlivých konfiguračních prvků. Nabízíme i implementaci doporučení, které vám na základě výsledků z námi provedených testů vystavíme, eliminujeme tak nalezené slabiny a zvyšujeme obranyschopnost při nenadálém reálném útoku.

Cloud
Migrace firemní infrastruktury do cloudového prostředí se stává trendem. Klíčovou roli představuje konfigurace cloudových služeb, ať už nativních, nebo služeb třetích stran. Konfigurační nedostatky mohou vést ke ztrátě firemních dat i důvěry zákazníků, proto jsme připraveni vám s otázkou bezpečné konfigurace vašeho cloudového prostředí pomoci.

Testy sociálním inženýrstvím

Sociální inženýrství je akt, ve kterém se sociální inženýr pokouší přimět svůj cíl k provedení akce, která nemusí být v nejlepším zájmu daného subjektu. Zaměstnanci jsou považováni za nejslabší článek bezpečnosti ve společnosti. Útočník tak může využít sociální inženýrství k prolomení i těch nejzabezpečenějších perimetrů. Sociální inženýři k tomu využívají útoky jako například vishing, phishing, nebo fyzickou infiltraci pomocí impersonace. Naším cílem je prověřit zabezpečení vaší společnosti za pomocí těchto metod a následně navrhnout nejlepší řešení, pro eliminaci nalezených rizik.

Penetrační testy infrastruktury

Interní
Při penetračních testech interní infrastruktury mapujeme vnitřní síť společnosti, identifikujeme aktivní síťové prvky a prověřujeme jejich bezpečnost. Pokoušíme se prolomit vybrané systémy a kompromitovat doménu společnosti eskalací privilegií z běžného uživatele na doménového administrátora. Součástí jsou také testy z pracovní stanice běžného uživatele.

Externí
Při penetračních testech externí infrastruktury klademe důraz na odhalení všech dostupných síťových služeb, komponent a jejich detailní enumeraci. Sběr veřejných informací o síťové infrastruktuře společnosti je pro útočníka klíčový. K tomuto účelu využíváme jak automatizované, tak vlastní proprietární nástroje a metodiky.

Zátěžové
Útočníci často u klíčových webových aplikací poškozují weby společností tím, že je jednoduše znepřístupní. Čím déle není uživatelům daná webová aplikace dostupná, tím větší jsou ztráty. V rámci Denial of Service testujeme vybrané služby, aby k těmto situacím nedocházelo a kritické webové aplikace tak fungovaly i při neočekávaně vysoké zátěži.

IoT
Naším hlavním zaměřením při testování internetu věcí (IoT) je zjištění, jak jednoduchým cílem daná zařízení jsou. Jaké informace z nich lze získat, a jak detekovat jejich zranitelnosti, které mohou být zneužity pro získání neautorizovaných přístupů či krádeží dat.

Wifi sítě
Penetračními testy Wi-Fi technologií simulujeme útok na přístup do vnitřní sítě organizace prostřednictvím bezdrátového signálu Wi-Fi sítí. Po získání přístupu prověříme kvalitu filtrování provozu mezi síťovým segmentem Wi-Fi klientů a zbytkem interních sítí. Do testů zahrnujeme i analýzy konfigurace připojení k bezdrátové síti na straně klientských zařízení.

SCADA
Zajistíme, aby byly vaše řídící systémy (SCADA) zabezpečeny před vnějšími i vnitřními hrozbami za pomocí penetračních testů. SCADA systémy jsou velmi často zastaralé a plné zranitelností, snadno se tak stávají terčem APT útoků. Mnoho systémů není aktualizováno, ze strachu z nefunkčnosti či zastavení výroby, tyto nedostatky pak mohou útočníci snadno zneužít k jejich ovládnutí.

VoIP
Zajišťujeme penetrační testy na veřejně dostupnou kritickou infrastrukturu organizace, jako jsou telefonní systémy VoIP. Pomocí metody man-in-the-middle odposlouchávají útočníci komunikaci mezi příchozím a odchozím připojením telefonů. Mohou tak získat přístup k choulostivým datům v interní síti VoIP. Prověříme všechna slabá místa, aby ve vaší organizaci k takovým situacím nedocházelo.

Specializované testy a služby

ATM

Prověříme zranitelnosti bankomatů během jednoho týdne. Naše komplexní analýza zahrnuje způsoby fyzického přístupu, eskalaci privilegií, testy operačního systému a aplikací. Můžeme se však soustředit pouze na penetrační testy infrastruktury, integračních služeb a managementu, reverzní analýzu softwaru, případně bezpečností analýzu zdrojového kódu.

Reverse Engineering

Při reverzním inženýrství zpětně analyzujeme funkčnosti testovaných aplikací, bez přístupu, či znalosti jejich zdrojových kódů a tím ověříme jejich odolnost vůči možným reálným útokům. Při analýze kódů využíváme zkušenosti z penetračních testů desktopových klientů.

Phishing

Testujeme odolnosti firem proti útokům vyděračskými programy. Při prověřování analyzujeme stávající situace včetně testu odolnosti systému. Výstupem je report s doporučeními příslušných řešení.

Codebashing

Pokud vyvíjíte aplikace, nabízíme vám prostřednictvím služby Codabashing řešení pro edukaci a evangelizaci v oblasti aplikační bezpečnosti. Ta umožňuje bezpečnostním a vývojovým týmům vytvářet a udržovat kulturu bezpečného vývoje. Prostřednictvím komunikačních nástrojů, gamifikace, vzájemných výzev a průběžných hodnocení vám Codebashing pomůže eliminovat vznik softwarových zranitelností ve zdrojovém kódu.

Ransomware

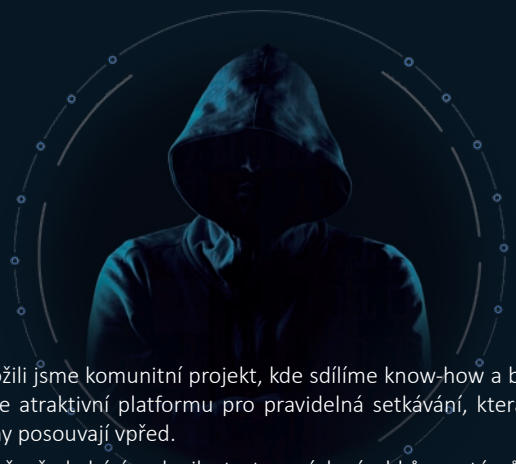
Nabízíme unikátní službu na test odolnosti vaší organizace vůči ransomware. Dokáže vaše bezpečnostní technologie či mechanismy odhalit tento typ malwaru? Jsou vaši zaměstnanci dostatečně proškoleni, aby ransomware nespustili ve vaší síti? To všechno vám řekneme.

RFID

U RFID technologií replikujeme veřejně známé útoky na konkrétní typy karet a rovněž se pouštíme do vlastního průzkumu možných slabých míst a potenciálních vektorů útoku.

Red Teaming

S Red Teamingem jdeme daleko za hranice klasických penetračních testů tím, že věrně simulujeme útoky reálných hackerských skupin a snažíme se ověřit komplexní zabezpečení organizace nejen v technologické oblasti, ale také na úrovni interních procesů a interních bezpečnostních specialistů. Na rozdíl od penetračních testů, kdy je po zadavateli běžně vyžadována určitá míra součinnosti, provádíme Red Teaming jako blackbox – veškeré informace o cíli zjišťujeme až v průběhu akce a snažíme se zůstat v utajení po co nejdelší dobu.



Založili jsme komunitní projekt, kde sdílíme know-how a budujeme atraktivní platformu pro pravidelná setkávání, která své členy posouvají vpřed.

Záměrně obcházíme logiku testovaných výrobků a systémů. Nabouráváme jejich procesy, hledáme zranitelnosti, chyby v implementaci a zabezpečení.

Zapojte se do programu testování zabezpečení IoT zařízení

Vaše zařízení podrobíme analýze a nalezené bezpečnostní zranitelnosti popíšeme v detailním reportu s návrhy na jejich odstranění.

Ozvěte se nám, pokud jste

- výrobci IoT a smart technologií
- prodejci, kteří chtějí svým zákazníkům nabídnout kvalitní servis
- uživatelé, kteří si nejsou jistí kvalitou zabezpečení zakoupeného produktu

Pro více informací o HackingLabu, komunitě a možnostech spolupráce navštivte náš web.

hackingLab hackinglab.cz

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