Penetrační testy Wi-Fi sítí

AEC

Součástí infrastruktury každé větší společnosti musí být v dnešní době i bezdrátová síť, která dovoluje zaměstnancům konektivitu z laptopů nebo mobilních zařízení z libovolného místa budovy. Bezdrátové sítě však také poskytují nové vektory útoků pro potenciálního útočníka s cílem kompromitovat zaměstnance nebo interní síť společnosti.

Penetrační testy pomůžou odhalit možné slabiny nebo konfigurační nedostatky v těchto sítích, které mohou být následně dle doporučení odstraněny co útočníkům znemožní tyto vektory zneužít a zvýší bezpečnost a odolnost sítě vůči reálnému kybernetickému útoku.

www.aec.cz

Z důvodu, že útočník se pro přístup k bezdrátové síti nemusí nacházet bezprostředně v budově společnosti ale jenom v dosahu sítě, jedná se o kritickou část pro zabezpečení.

Penetrační testy Wi-Fi technologií simulují útok na přístup do vnitřní sítě organizace prostřednictvím bezdrátového signálu Wi-Fi sítí. Po získání přístupu bude prověřena kvalita filtrování provozu mezi síťovým segmentem Wi-Fi klientů a zbytkem interních sítí.

Součástí testů je také analýza konfigurace připojení k bezdrátové síti na straně klientských zařízení. Výstupem testu bude přehled a zmapování provozovaných Wi-Fi sítí a seznam bezpečnostních nálezů s následným dopadem na vnitřní sít organizace.

Realizace penetračních testů zahrnuje zejména následující kategorie:

- Mapování a analýza dostupných Wi-Fi sítí v areálu společnosti.
- Detekce možných Rogue AP.
- Prověrka zaměstnaneckých Wi-Fi sítí.
- Pokus o získání přístupu.
- Analýza filtrování mezi Wi-Fi a LAN segmenty sítě.

Penetrační testy Wi-Fi sítí

Mapování a analýza dostupných Wi-Fi sítí v areálu společnosti

Cílem je zmapování a analýza dostupných Wi-Fi sítí uvnitř areálu společnosti. Analýza je zaměřena na zmapování jednotlivých Access pointů a použití technologických a kryptografických mechanizmů použitých k zabezpečení autentizace a přenášených dat.

Detekce možných Rogue Access Point (AP)

Jako Rogue Access Point (AP) je označován neautorizovaně nasazený Access Point v prostorech a nejbližším okolí společnosti. Rogue AP bývá útočníkem nejčastěji nasazen s cílem útoku na zabezpečení stávající bezdrátové sítě – v takovém případě útočník duplikuje nastavení cílové sítě. Druhou častou možností je nasazení otevřené bezdrátové sítě s cílem následného útoku vůči připojeným stanicím či cílem odposlechu přístupových údajů.

Prověrka návštěvnických Wi-Fi sítí

Fáze má za cíl analyzovat zabezpečení návštěvnických Wi-Fi sítí. Tyto sítě jsou obvykle nakonfigurovány s otevřeným přístupem a autentizací pomocí captive portálu nebo se zabezpečením typu Personal (WEP, WPA-PSK s TKIP, WPA2-PSK s CCMP).

Prověrka zaměstnaneckých Wi-Fi sítí

Fáze má za cíl analyzovat zabezpečení zaměstnaneckých Wi-Fi sítí. Tyto sítě jsou obvykle nakonfigurovány jako WPA Enterprise s autentizací dle standardu 802.1X, výjimečně pak se zabezpečením typu Personal (WEP, WPA-PSK s TKIP, WPA2-PSK s CCMP).

Pokus o získání přístupu

Postup útoku s cílem získání neautorizovaného přístupu se liší dle použitého zabezpečení sítě. Existují různé známé útoky na zabezpečení WEP, WPA-PSK, WPA2-PSK nebo WPA-Enterprise, které jsou během této fáze testovány. Pro zabezpečení WEP existuje mnoho zdokumentovaných útoku jako KoreK chop-chop attack, Fragmentation Attack, ARP-request replay attack a další.
Pro WPA2-PSK to může být například offline prolamování sdíleného hesla nebo zneužití povolené WPS metody autentizace. V případě WPA-Enterprise s použitím autentizace dle standardu IEEE 802.1X je síť prověřována na výskyt slabých autentizačních metod (EAP-MD5, Cisco LEAP). Je zde ověřena správná konfigurace a hardening sítě a klientských zařízení. Dále jsou zkoumány možnosti odchycení citlivých dat jako uživatelských jmen nebo hesel.

Analýza filtrování mezi Wi-Fi a LAN segmenty sítě

V této fázi dochází k autorizovanému přihlášení do všech testovaných Wi-Fi sítí společnosti pod poskytnutými uživatelskými účty. Následně je prověřována důslednost oddělení síťového segmentu Wi-Fi klientů od jiných citlivých segmentů sítě (DMZ, produkce, …). V případě přítomnosti různých VLAN je taktéž prověřeno výše uvedené.

Naše přednosti

- Patříme mezi zavedené české security firmy, na trhu úspěšně působíme již déle než 30 let.
- Máme více než 10 let zkušeností na poli bezpečnosti infrastruktury a bezdrátových sítí.
- Široký tým certifikovaných etických hackerů se zkušenostmi z několika desítek provedených penetračních testů ročně.
- Jsme držiteli certifikací eMAPT, CISSP, OSCP, OSCE, CEH a celé řady dalších.
- Provozujeme vlastní hackerskou laboratoř na výzkum i v oblasti různých druhů bezdrátových sítí.
- Naslouchámе klientům a přizpůsobujeme testy jejich potřebám a časovým možnostem.
- Sledujeme moderní trendy v oblasti bezpečnosti bezdrátových sítí.
- Při testování klademe důraz na manuální přístup, který vede k odhalení většího množství chyb a minimalizaci false-positive nálezů.

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