

## Penetrační testy

Prověřte úroveň zabezpečení systémů a aplikací organizace dříve, než to udělá někdo jiný!

Penetrační testy simulací útoku hackera na síťové i aplikační úrovni prověří schopnost systémů organizace odolávat reálným kybernetickým útokům z vnějšího prostředí, ale také schopnost odolat neautorizovaným zásahům zaměstnanců, a to bez ohledu na to, jestli jednájí vědomě, nebo se pouze dopustí chyby.

Penetrační testy pomohou odhalit nedostatky v návrhu systému a jeho architektuře a identifikovat výkonnostně poddimenzované prvky systému.

Penetrační testy ověří míru zajištění důvěrnosti, integrity a dostupnosti dat zpracovávaných elektronickými systémy, a tím zajistí bezproblémový chod ICT organizace a souvisejících business procesů.

### Nabízené služby

#### Penetrační testy infrastruktury

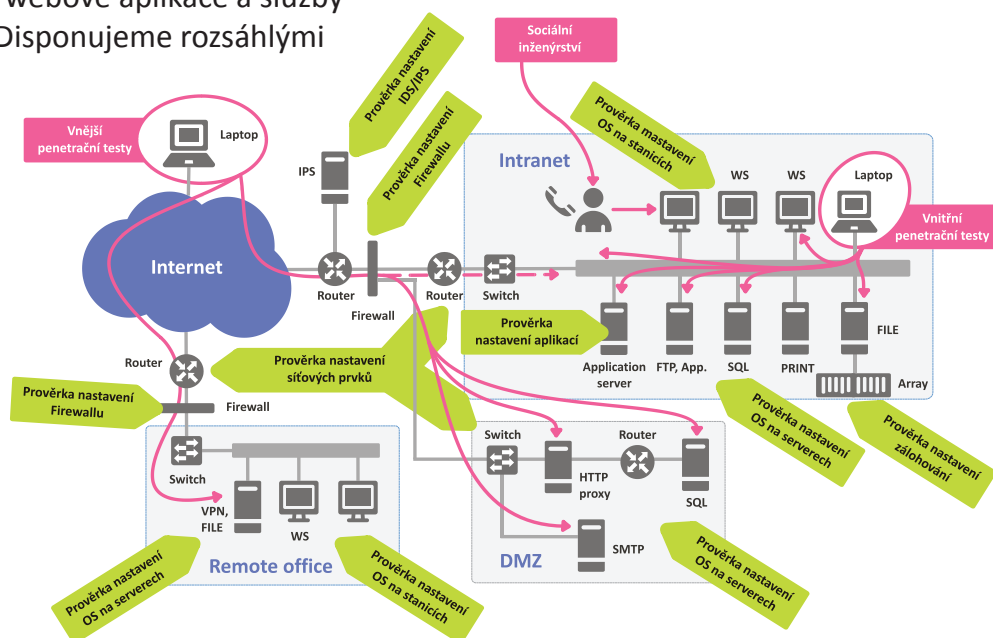
Detailní prověrka zabezpečení všech komponent počítačové sítě společnosti dostupných ze sítě internet nebo z interní sítě společnosti. Prověření organizace provádíme z pohledu útočníka, který má k dispozici pouze veřejně dostupné informace nebo již získal přístup k interním systémům uvnitř organizace s cílem simulovat interního uživatele nebo malware.

#### Penetrační testy aplikací

Provádíme prověrky bezpečnosti aplikací od jednoduchých statických portálů až po složité webové aplikace a služby s pokročilou business logikou. Disponujeme rozsáhlými zkušenostmi s testy nativních mobilních aplikací pro platformy Android, iOS a Windows. Naši specialitou jsou desktop aplikace typu „tlustý klient“, které jsou často z bezpečnostního hlediska opomíjeny. Mimo nezbytné automatizované testy se soustředíme na manuální testování, které zahrnuje složité komunikační vazby technologií a business logiku aplikací.

### Naše řešení

- Více jak 20 let zkušeností na poli bezpečnosti v České a Slovenské republice.
- Široký tým certifikovaných specialistů se zkušenostmi ze stovek provedených penetračních testů kritických aplikací a rozsáhlých systémů.
- Klademe důraz na manuální přístup při testování, což má za následek odhalení většího množství chyb zejména v business logice aplikací.
- Vyhodnocení úrovně zabezpečení ICT společnosti a definice reálných rizik v kontextu předpokládaného dopadu na business.



## Penetrační testy bezdrátových sítí Wi-Fi

Komplexní prověrka návrhu bezdrátové sítě a úrovně zabezpečení jejích jednotlivých komponent a souvisejících systémů zahrnuje mimo jiné: pokusy o průnik a odposlech, měření přesahů, detekce neoprávněných AP či analýzu prostupnosti sítí.

## Penetrační testy mobilních zařízení

Detailní analýza návrhu architektury pro mobilní komunikaci v rámci firmy i mimo ni. Vyhodnocení úrovně zabezpečení jednotlivých mobilních zařízení ve vztahu k jejich uživatelům i k dalším aktivům společnosti.

## Penetrační testy VoIP

Prověrky systémů pro hlasovou komunikaci přes počítačové sítě. Kromě testů běžných pro síťová zařízení jsou prověřována i specifika komunikační služby s dopadem na důvěrnost, dostupnost a integritu přenášených informací.

## Penetrační testy řídicích a kontrolních systémů (SCADA)

Testy počítačových sítí napojených na komponenty pro řízení a monitoring technologických zařízení v průmyslu. Prověrka odhalí zejména slabá místa v návrhu architektury a bezpečnosti jednotlivých komponent kontrolního a řídicího systému, která mohou mít za následek provozní výpadky, a tak i finanční ztráty.

**Veškeré penetrační testy a audity jsou prováděny dle vlastní metodiky pro provádění penetračních testů, která vychází z obecně platných standardů, doporučení a metodik pro provádění bezpečnostních prověrek (OWASP, OSSTMM, PTES, NIST a dalších) a která vznikla na základě dlouholetých zkušeností specialistů AEC.**

## Další služby nabízené jako doplněk k penetračním testům

### Testování DoS (Denial of Service)

Testování odolnosti systému proti útokům směřujícím k odepření služby poskytované systémem.

### Školení hacking

Školení administrátorů zákazníka o metodách a nástrojích používaných hackery za účelem lepšího pochopení uvažování útočníků a způsobu jejich útoků s cílem uplatnit tyto informace pro zvýšení úrovně jimi spravovaných systémů.

### Prověrky na základě definovaných metodik

Testy a prověrky systémů vycházejících z požadavků na shodu s definovanou metodikou, například PCI-DSS, SOX a další.

[www.aec.cz](http://www.aec.cz)

## Reference

- Pokud máte zájem zjistit více o tom, jak pracujeme, neváhejte se na nás zeptat v některé z následujících společností. Jedná se pouze o vybrané a schválené reference z poslední doby.
- Zuno bank, AG – banka si nás vybrala jako spolehlivého partnera pro svůj start na trhu. Provedli jsme kompletní testy všech kritických systémů této banky.
- ING bank, a.s. – provedli jsme rozsáhlé penetrační testy IS ING, a to nejen pro ING Česká republika.
- Pravidelně testujeme bezpečnost pro zákazníky, jako jsou T-Mobile, Komerční banka, Česká spořitelna, ČSOB, Volksbank či Poštová banka.

AEC, spol. s r.o.  
Purkyňova 2845/101  
612 00 Brno, Czech Republic  
Phone: +420 530 507 200  
Fax: +420 530 507 220

AEC, spol. s r.o.  
European Business Center  
Dukelských hrdinů 34  
170 00 Praha 7, Czech Republic  
Phone: +420 267 311 402  
Fax: +420 266 177 155

**AEC**

DATA SECURITY