VersaSecurity
part of Versa Systems

Bezpečnostní testy

Bezpečnostní test nabízí neocenitelný a přesvědčivý způsob, jak provést posouzení aktuálního stavu bezpečnosti ICT organizace tak, jak se jeví navenek vůči externím útočníkům. Detailně popisují zjištěné nedostatky a poskytují tak rady a návrhy řešení k odstranění těchto slabých míst a posilují celkovou bezpečnostní strategii organizace.

Testy bezpečnosti ověřují skutečnou úroveň bezpečnostních opatření a simulují skryté síťové útoky tak, aby bylo možné identifikovat specifické zranitelnosti Vaší síťové infrastruktury a odhalit potenciální nechtěné přístupy k citlivým informacím. Jsou-li tato zranitelná místa objevena včas, může na ně být patřičně reagováno, čímž je sníženo riziko využití takového zranitelného místa externím útočníkem a dosaženo zvýšení úrovně bezpečnosti síťové infrastruktury.

Prostřednictvím kvalifikovaně provedených bezpečnostních testů dle mezinárodně platných standardů (ISO 27001, OSSTMM, OWASP, ISSAF a další) ověří úroveň Vaší bezpečnosti a pokusíme se simulovaným útokem získat přístup k vašemu on-line majetku a firemním zdrojům prostřednictvím síťových serverů, prvků, stolních počítačů a notebooků. Takové testy jsou prováděny ve dvojí rovině, buď z interního nebo externího pohledu, stejně jako by byl prováděn skutečný útok na vaše data a informace.

Testy, které poskytujeme

- Penetrační testy
- Testy technických zranitelností
- Audit procesů řízení bezpečnosti
- Softwarový audit

Standardy použité při testech

- ISO/IEC 27001
- OSSTMM
- OWASP
- ISSAF

> “ Bezpečnost organizace je tak silná, jak silný je její nejslabší článek.

5 důvodů proč provést bezpečnostní test

- Poskytne vhodný výchozí bod. Bezpečnostní test poskytuje první krok k pochopení současného stavu bezpečnosti ICT v organizaci.
- Vytvoří přesvědčivé důkazy. Správně dokumentované výsledky bezpečnostních testů dají jasnou zprávu o náchylnosti zákaznických dat, personálních údajů, nebo dokonce e-mailových účtů managementu k zneužití.
- Provádí nezávislý audit. Bezpečnost opatření je třeba nezávislým pohledem přezkoumávat systematicky a pravidelně vzhledem k vývoji nových internetových hrozeb.
- Chrání před riziky plynoucími ze spolupráce s třetími stranami. On-line obchod vyžaduje, aby organizace poskytovala partnerům, dodavatelům a dalším subjektům třetích stran důvěryhodné připojení do svých sítí.
- Provede ověření současného stavu. Bezpečnostní test poskytuje ověření propojení mezi podnikatelskými aktivitami a bezpečnostním rámcem, který umožňuje úspěšné plnění obchodních plánů s minimálními riziky.