SNIŽTE BEZPEČNOSTNÍ RIZIKA POMOCÍ PENETRAČNÍCH TESTŮ

ODHALTE SLABINY DŘÍVE, NEŽ TO UDĚLAJÍ JINÍ

Penetrační testy jako jedna z forem tzv. etického hackingu, pomohou ověřit, jak by obstály firemní systémy a celkově nastavené bezpečnostní politiky v případě reálného hackerského útoku. Ověří úroveň bezpečnosti systémů organizace a odolnost informačních a komunikačních technologií. V mnoha případech je to také povinný požadavek na dodržování předpisů nebo průmyslových standardů.

PŘESTĚHOVALI JSTE SE DO NOVÉ LOKALITY? NASADILI JSTE NOVÝ SYSTÉM?

Proveďte preventivní penetrační test! Každý zásah do nastavení firemních systémů nebo zařazení nového prvku může potenciálním útočníkům otevřít dveře k průniku do firemní infrastruktury.

ZAZNAMENÁVÁTE VE VAŠEM OKOLÍ ZVÝŠENÝ POČET ZPRÁV O POKUSECH O NAPADENÍ?

S velkou pravděpodobností byste mohli být v hledáčku hackerů i vy. Máte jistotu, že jste nebyli už před časem také napadeni? Je to ten pravý čas k provedení penetračního testu.

287 dnů

(VÍCE NEŽ 9 MĚSÍCŮ)

BYLA V ROCE 2021 PRŮMĚRNÁ DOBA DETEKCE A ZABRÁNĚNÍ ÚNIKU NEBO NARUŠENÍ DAT[1)]

Zdroj: 1. IBM Security – Cost of a Data Breach Report 2021

ODBORNÁ ASISTENCE POMŮŽE PODÍVAT SE JINOU OPTIKOU

Pro boj s hackery je potřeba myslet jako hacker. I když má interní IT tým zkušenosti s bezpečnostním testováním a používá vlastní nástroje pro testování, třetí strana provádějící kontrolované penetrační testování s větší pravděpodobností odhalí trhliny, které by interním kontrolám mohly uniknout. Pokusem o prolomení zabezpečení systému za použití stejných nástrojů, které by mohl mít k dispozici protivník, je možno ověřit skutečnou funkčnost a vzájemnou součinnost všech technických kontrol, zásad a postupů.

CO MŮŽETE OČEKÁVAT OD NÁS:

Pochopíme bezpečnostní rizika vašeho podnikání a následně vystavíme váš systém nebo IT projekt profesionálně vedenému útoku tak, jak by mohl reálně probíhat. Díky tomu odhalíme slabá místa systému a navrhneme postupy, jak je posílit.

ZPŮSOB REALIZACE

Testy provádíme v následujících, na sebe navazujících fázích:

- **SHROMAŽĎOVÁNÍ INFORMACÍ**
  získání maxima informací o testovaném systému neinvazivními metodami
- **IDENTIFIKACE POTENCIÁLNÍCH ZRANITELNOSTÍ**
  využití invazivních metod získávání informací o testovaném systému
- **TESTOVÁNÍ REÁLNÝCH MOŽNOSTÍ ZNEUŽITÍ**
  Užití zjištěných zranitelností k získání částečné či plné kontroly nad systémem / aplikací.

VARIANTY PROVEDENÍ

Nenabízíme univerzální řešení, protože ani vaše potřeby nejsou univerzální. Každý z penetračních testů je proto tvořen přímo na míru vaší IT infrastruktury a pokrývá široké spektrum bezpečnostních zranitelností. Od veřejně známých, až po útoky navržené přímo pro prolomení vašich systémů. Příkladem prováděných typů testů podle testovaných systémů mohou být např:

- **Externí nebo interní testy celkové IT infrastruktury**
- **Testy webových aplikací**
- **Test mobilních aplikací**
- **Testy API rozhraní**
- **Test IoT, ICS/SCADA**
- **Testy WiFi bezdrátových sítí**
- **Testy bezpečnosti fyzických zařízení**
- **Zátěžové testy odolnosti proti DDoS útokům**

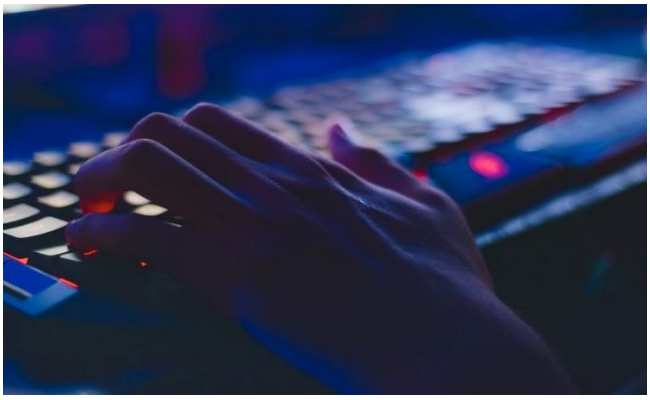
Výsledky shrneme do **SOUHRNNÉ ZPRÁVY** složené ze čtyř samostatných kapitol:

Úvodí kapitola nabídne krátkou **rekapitulaci** rozsahu provedeného auditu a detaily o jeho exekuci.

Druhá kapitola, nazvaná **Manažerské shrnutí**, prezentuje čitateli ucelený expertní výrok o úrovni bezpečnosti testované instance.

Kapitola **Nálezy** penetračního testu obsahuje výčet nalezených zranitelností seřazených podle jejich závažnosti.

Poslední kapitola zprávy **Detailní popis nálezů** poskytne pro každou zranitelnost následující informace: popis, dopad, závažnost, návrh způsobu odstranění, doplňující technické informace.



VE VÝSLEDKU...

- **Zjistíte**, zda jsou bezpečnostní politiky nastavené ve vaší organizaci opravdu účinné
- **Ověříte si**, zda vaše systémy nebyly již před časem napadeny a nedochází k únikům dat
- **Objevíte** případná slabá místa, o kterých jste možná neměli tušení a budete se moci zaměřit na jejich posílení

PROČ BYSTE SI MĚLI VYBRAT PRÁVĚ NAŠE ŘEŠENÍ.

Testovací proces jsme shopni doplnit vlastním bezpečnostním poradenstvím s využitím znalostí a dlouhodobých zkušeností našeho expertního týmu.

Thein Security patří k průkopníkům kybernetické bezpečnosti se zaměřením na **prevenci úniku citlivých dat**, obrany proti **sofistikovaným útokům**, detekce neznámého **malwaru** a aktivní ochrany proti **útokům DDoS**. Dodáváme služby a technologie do **hybridních prostředí** (on prem / cloud) a specializujeme se na **Zero Trust přístup.**

STANEME SE VAŠÍM PARTNEREM PRO OBLAST KYBERNETICKÉ BEZPEČNOSTI.

Pro více informací o Penetračním testování a dalších službách kontaktujte naše obchodní zástupce na obchod.security@thein.eu nebo navštivte naše webové stránky.

Thein Security s.r.o., Pikrtova 1737/1a, 140 00 Praha 4 – Nusle, e-mail: info.security@thein.eu
Společnost vedená u Městského soudu v Praze oddíl C, značka 109813, IČO: 27415546, DIČ: CZ27415546