Jak si vedou české firmy v penetračních testech

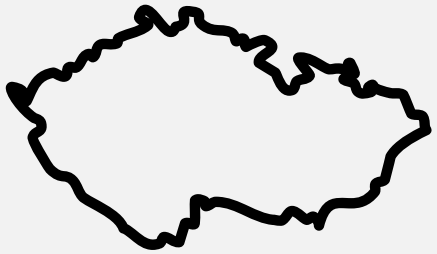
Konference Kybernetická bezpečnost XI

4. 10. 2023

Peter Šinaľ
CEO & Head of Consulting
Trusted Network Solutions

TRUSTED NETWORK SOLUTIONS

TNS – Trusted Network Solutions



Česká společnost

Penetrační testy
a testy odolnosti
uživatelů

Kernun
INTERNET SECURITY

Adaptivní
databáze hrozeb

Penetrační testování

Cílená aktivita pro identifikaci zranitelných míst v organizaci

Oboustranně odsouhlasené podmínky

Možnost modelovaní chování útočníka

Ověření nastavených politik – Firewall, WAF, SOC, EDR

Demonstruje reálné důsledky – pokus o exploitaci

V porovnaní s red-teamingem se dokáže zaměřit na konkrétní aplikaci nebo část infrastruktury

Infrastruktura – technologie

Externí infrastruktura:

- Neaktualizované SW vybavení
- Podpora TLS 1.0/1.1
- Nebezpečná autentizace

Interní infrastruktura:

- Považována za méně dosažitelnou útočníky, a proto lze ve většině případů získat administrátorský přístup k LDAP a NTLM otiskům hesel
- Neprovádění aktualizací a obecně management aktiv
- Dostupné citlivé údaje – konfigurace, zálohy, otisky hesel

Infrastruktura – fyzická vrstva

Zabezpečení na fyzické vrstvě je možné lehce překonat

Nejdříve selže recepce nebo zaměstnanci

Zranitelné jsou i přístupové karty, náchylnost ke kopiím

802.1X-2004 i verze 2010 jsou zranitelné vůči útokům typu Man-in-the-Middle, kdy je možné toto zabezpečení obejít

Aplikace

Zaměření pouze na vlastní produkty nebo produkty vyvíjených na míru

Absence auditů/testů na úrovni OS/DBMS

Největší problém je autorizace akcí uživatelů

Chyby v designu – enumerace uživatelských jmen, možnost blokace, absence ochrany vůči brute-force

Zastaralé komponenty a knihovny

Bezdrátové sítě

Captive portály představují větší riziko než zabezpečení heslem, protože řízení přístupu je často pouze na základě MAC adresy.

WPA2-Enterprise ověřením přes Radius – náchylné k útokům typu evil-twin, kdy útočník získá otisky hesel netNTLM. Prolomení netNTLM otisku hesla je výrazně jednodušší než WPA2 otisku hesla.

Stále vyskytující se chybou je neoddělení návštěvnické sítě od interní infrastruktury.

Amatéři útočí na firmy, profesionálové na lidi

Peter Šinaľ, CEO

tns TRUSTED NETWORK SOLUTIONS

Uživatelé

Testování odolnosti uživatelů není věnována taková pozornost jako testování technologií. Poměr na úrovni 3:1

Náchylnost uživatelů se dlouhodobě pohybuje na úrovni > 30 %

Většina uživatelů neví o možnosti podvržení telefonního čísla

Řada správců nemonitoruje svoji hlavní doménu

Shrnutí

Penetrační testy neodhalují jenom zranitelnosti, ale také chyby v politikách nebo poukazují na jejich porušování

V infrastruktuře je problémem aktualizace aktiv a příliš velké spoléhání se na fyzickou ochranu

V případě aplikací je problémem autorizace rolí a chybí také audity OS, DBMS,

Velkým rizikem jsou uživatelé, kterým se nevěnuje pozornost