ALEF Training center

(Ne)veselé historky z bezpečnostního testování

Michal Zedníček
Head of CyberSecurity Business Consulting
michal.zednicek@alef.com
+420 602 578 443

5 bezpečnostních testů

Test1
Test webové aplikace

Test2
Test fyzické bezpečnosti

Test3
Test krádeže dat

Test4
Vishing

Test5
Phishing

404 Autorizace Not Found

- Penetrační test webové aplikace

Co se stalo

- Dodavatel po nasazení aplikace zapomněl zapnout autorizaci uživatelských akcí.
- Uživatelé si tak mohli dělat, co se jim zachce – měnit si hesla, zamykat účty, nebo dokonce zakládat administrátorské účty.
- Získání admin účtu k testované aplikaci během 3 minut je překvapením i pro potenciálního útočníka

Fyzická krása vs. fyzická bezpečnost

- Test fyzické bezpečnosti do chráněných prostor
- Měli jsme za úkol proniknout jakýmkoliv způsobem do chráněných prostor
- Neobvykle odolné vstupní mechanismy

Co se stalo:

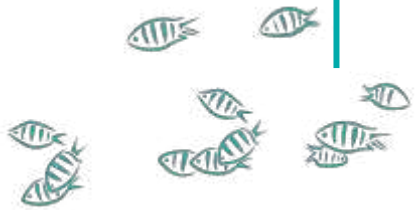
- Psychologie: Plaz/Savec/Neokortex
- Krásná dáma ve výrazných červených šatech s oslňujícím úsměvem
- Zaměstnanci muži ji rádi považovali za „svou“ – zdravili, otevírali dveře a pustili ji úplně všude

Co dělají IT admini s vyřazenými PC

- Test procesu likvidace dat

Co se stalo:

- V rámci akademického testu jsme se zaměřili na výrobní podniky
- Zkusili jsme v bazarech najít Pcčka z výrobních podniků a obnovit na nich data
- Získali jsme nejenom business model podniku, ale i peprnou soukromou komunikaci



Vishing

- Testování procesů HR a bezpečnostního povědomí zaměstnanců HR

Co se stalo:

- Získali jsme ze sociální sítě osobní údaje jednoho zaměstnance (jméno, kde bydlí, v které pobočce pracuje …)
- Vydávali jsme se za tohoto zaměstnance, zavolali jsme na HR a navodili jsme emergency stav
- Podařilo se nám HR pracovníka přesvědčit k resetu legitimního účtu reálného zaměstnance
- HR pracovník byl ochoten přiřadit jako autentizační mechanismus naše telefonní číslo

Phishing

- Phishingová a baitingová kampaň

Co se stalo:

- Simulovaný škodlivý soubor odeslaný jednomu uživateli byl stáhnut 3 dalšími zaměstnanci na 5 různých PC
- 1 účet byl pod právy lokálního administrátora
- Zároveň jsme změnili nastavení REPLY hlavičky na jiný email – zaměstnanci nám posílali celou komunikaci, jak si simulaci škodlivého souboru rozesílali

Co ukazuje bezpečnostní testování

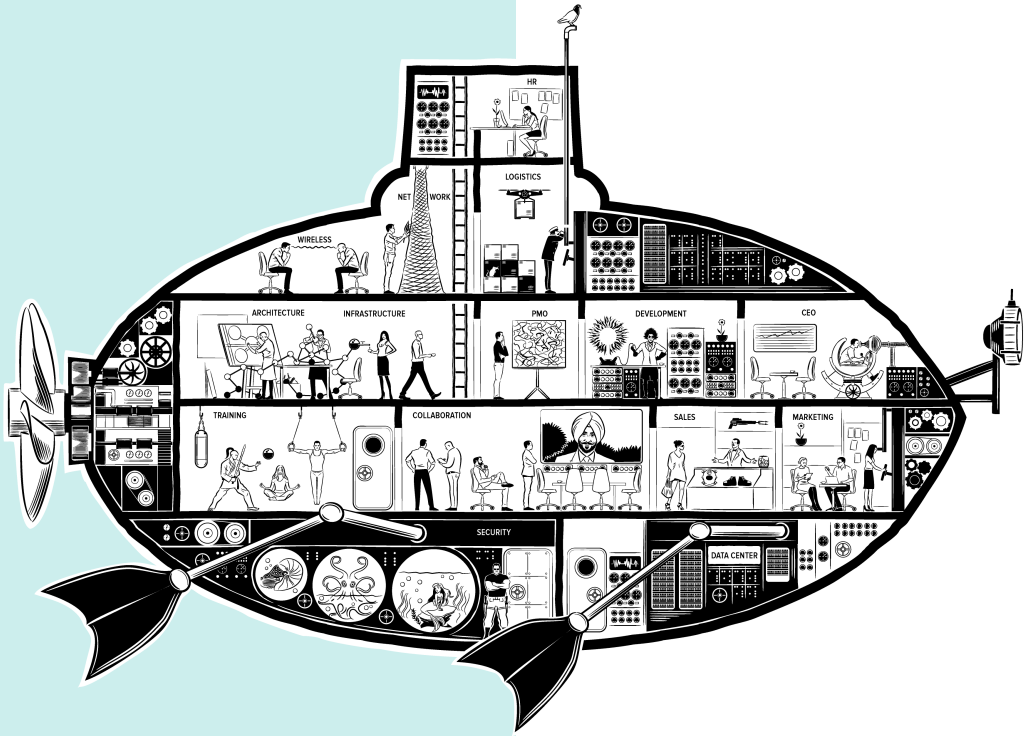
Že když NEVÍM, jak na tom jsem, je lepší provést obecnější techniku auditu (podrobného)

NĚKDY to může fungovat jako dobrý budíček

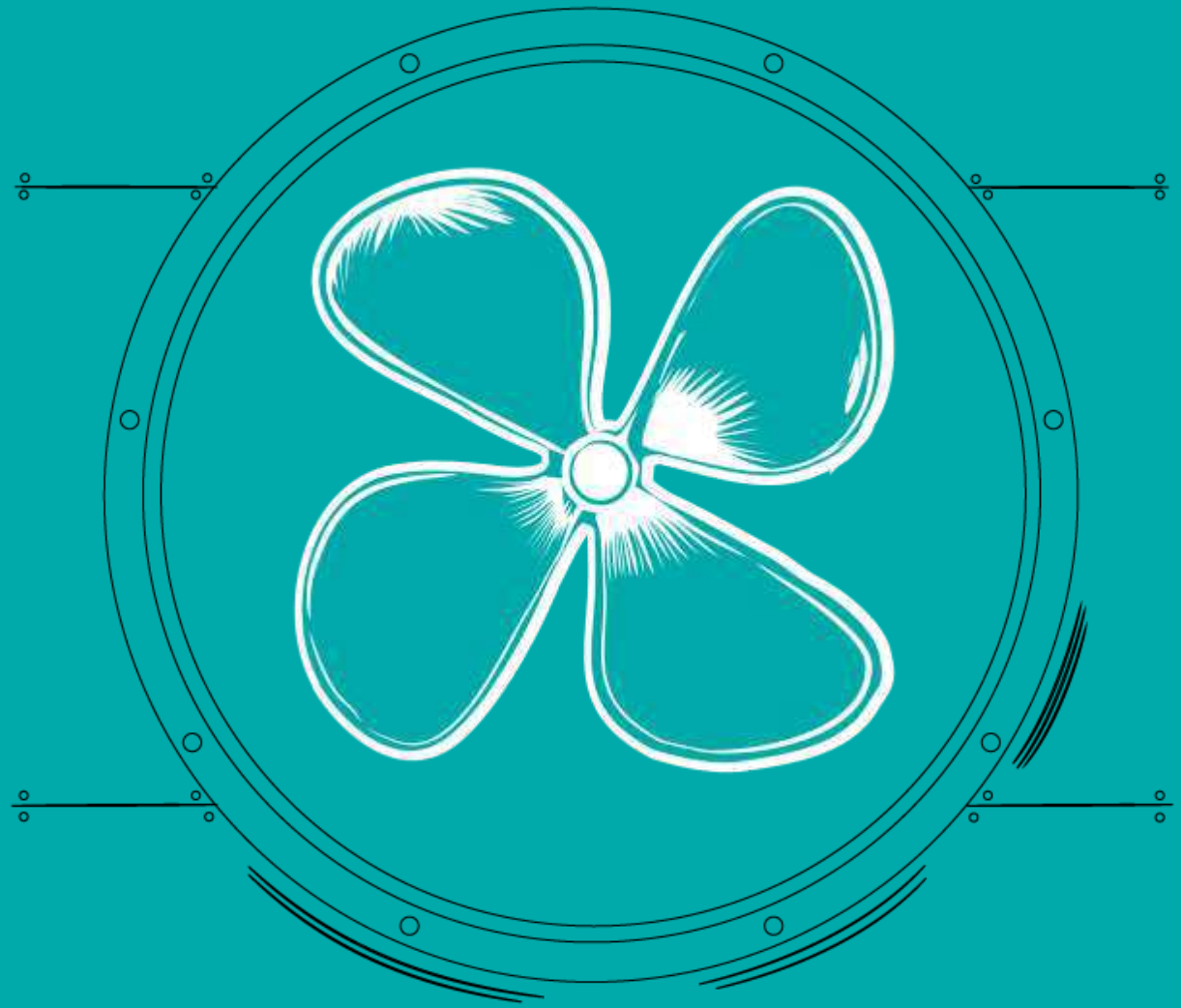
Jakmile použijeme techniku sociálního inženýrství, je úspěch TÉMĚŘ jistý

My v ALEFu jsme ti HODNÍ. Objednat nás znamená, že máte ODVAHU něco řešit

Trust the STRONG!



ALEF Training center



Thank you for your attention!