KONICA MINOLTA

MICROSOFT 365 ATTACK SIMULATOR: 4HODINOVÝ WORKSHOP

WORKSHOP (ON-LINE)

Žijeme v digitálním světě. Nejen naše pracovní, ale i osobní životy, dokonce i finance se začaly přesouvat do světa internetu, mobilních zařízení a elektronických médií. Bohužel nás to činí zranitelnější než kdykoli předtím. Útoky hackerů, invaze do soukromí, podvody a mnoho dalších nebezpečí se objevují každý den.

Obecným faktem je, že útoky hackerů a porušení bezpečnosti pravidelně ovlivňuje firmy všech velikostí. Tyto incidenty jsou často natolik významné, že se dostávají na přední stránky novin a způsobují nenapravitelné poškození pověsti zúčastněných společností.

Pokud ještě stále nemáte obavy o svou kybernetickou bezpečnost, měli byste.

Pravidla a nástroje kybernetické bezpečnosti nás chrání před hackery, kybernetickými zločinci a dalšími původci podvodu. **Tento workshop vám pomůže zvýšit povědomí o kybernetické bezpečnosti ve vaší organizaci.**

Pokud jste globálním administrátorem nebo security administrátorem a vaše organizace má Office 365 Advanced Threat Protection Plan 2, který zahrnuje funkce vyhledávání hrozeb a reakce na ně, můžete pomocí Attack Simulatoru spustit realistické scénáře útoků ve vaší organizaci. To vám může pomoci identifikovat zranitelná místa a najít rizikové uživatele dříve, než vás ovlivní skutečný útok zvenčí.

Office 365 ATP Plan 2 je součástí Office 365 E5, Office 365 A5 a Microsoft 365 E5 planů.

AGENDA

Úvod do simulátoru útoku

- Krátce vysvětlíme koncept Attack Simulatoru vašemu globálnímu nebo bezpečnostnímu administrátorovi.
- Společně projdeme dostupné bezpečnostní kampaně, připravíme je a spustíme ve vaší organizaci:

Spear phishingové kampaně

- Phishing je obecný pojem pro e-mailové útoky, snaží se ukrást citlivé informace ve zprávách, které se zdají být od legitimních nebo důvěryhodných odesílatelů. Spear phishing je cílený phishingový útok, který používá velmi soustředěný a přizpůsobený obsah, jenž je speciálně přizpůsoben cíleným příjemcům (obvykle po předchozím průzkumu útočníkem).

Kampaně k prolomení hesla

- Útok se pokouší uhodnout hesla uživatelských účtů v organizaci, obvykle poté, co útočník identifikoval jeden nebo více platných uživatelských účtů.

Výsledky kampaní

- Po dokončení kampaní si společně prohlédneme výsledky znázorněné v grafech, které budou obsahovat statistické údaje, jako je celkový počet oslovených uživatelů, počet úspěšných pokusů útoku, celková úspěšnost útoku, nejrychleji získané přihlašovací údaje apod.
- Naši odborníci vám vysvětlí získaná data a získáte doporučení, jaké další bezpečnostní opatření ve vaší společnosti zavést.

DÉLKA WORKSHOPU

4 hodiny

- on-line, rozděleno do několika samostatných schůzek

PŘEDPOKLADY

- Office 365 Advanced Threat Protection Plan 2
- Vzdálený přístup pro naše experty (sdílená obrazovka)

VÝSTUPY WORKSHOPU

- Zvýšíte povědomí o kybernetické bezpečnosti ve své organizaci.
- Získáte přehled o možnostech a nastavení nástroje Attack Simulator, jeho použití a výstupech.
- Obdržíte sadu doporučení našich expertů pro následné kroky vedoucí k zlepšení kybernetické bezpečnosti.

CENA WORKSHOPU

- **10.000 Kč** bez DPH

KONICA MINOLTA

Konica Minolta IT Solutions Czech a.s., U Plynárny 1002/97, 101 00 Praha 10, its@konicaminolta.cz, www.konicaminoltaits.cz