Školení IT bezpečnosti pro koncové uživatele (3-6h)

1. Zabezpečení hesel a proč už hesla nestačí
2. E-maily, phishing a jak poznat i jinde než v e-mailu
3. Sociální inženýrství, manipulace a jak nenaletět
4. Podvodné e-shopy a platby on-line
5. Bezpečnost mobilních zařízení
6. Bezpečnost sdílených záznamů, dat a cloudů
7. Tipy, triky a nástroje, které vám pomohou

Workshop IT bezpečnosti pro adminy a pokročilé (6h)

1. Zabezpečení hesel a proč už hesla nestačí, útoky na hesla, passkeys, 2FA a jak ho obejít
2. E-maily, moderní phishing a jak ho poznat i jinde než v e-mailu, ukázky, best practices v mailsecurity
3. Sociální inženýrství, manipulace a jak nenaletět, reálné casy a hračky jako Flipper Zero, Rubber Ducky, WiFi Pineapple, o.MG cable, DSTIKE watche…
4. Podvodné e-shopy a platby on-line, NFC relay útoky…
5. Bezpečnost mobilních zařízení, android malware, zero-days, GrapheneOS
6. IoT, vulnerability skeny, VPNky a spol
7. Tipy, triky a nástroje, které vám pomohou
8. Příručka v PDF s návody na doma a pro rodinu jako bonus

Ochrana soukromí na internetu (3h)

Při každodenních online aktivitách můžete odhalit osobní informace, které můžou jiní lidé či společnosti použít k ohrožení vašeho soukromí. Může se jednat o citlivé informace, jako je vaše IP adresa, e-mailová adresa, místo, kde se momentálně fyzicky nacházíte, nebo citlivé informace ze svého osobního i profesního života. Tyto údaje proti Vám mohou použít jak podvodníci, tak velké společnosti, které se sběrem dat živí. Jak se tomu bránit a své soukromí střežit se dovíte na školení, které povede Pavel Matějíček, odborník na kybernetickou bezpečnost.

1. Bezpečné www prohlížeče – které neshromažďují data o uživateli a vhodné doplňky
2. Vyhledávače respektující soukromí

3. Možnost zneužití fotografií, videí a metadat a jak se bránit
4. Propojení mobilu a sociálních sítí, personalizace a manipulace výsledků
5. Jak komunikovat bezpečně – e2e messengery
6. Nástroje pro zabezpečení výše uvedených bodů a šifrování
7. Zakrytí stop - IP adresa, DNS, VPN, TOR aneb jak se v tom vyznat
8. "Fenomén" G-mail a ANDROID v porovnání s APPLE (ochrana dat)
9. Alternativní operační systémy

OSINT – zjišťování informací z veřejných zdrojů (3h)

Myslíte si, že se toho o Vás nedá z internetu moc zjistit? Tak to se budete divit! Etický hacker Pavel Matějíček nám přijde ukázat, co vše se na nás dá vydolovat z hlubin internetu a jak tyto střípky informací poskládat do komplexního celku.

Kurz otevřeného zpravodajství (OSINT) poskytuje ucelený přehled o tom, jak shromažďovat a analyzovat informace z veřejně dostupných zdrojů. Kurz začíná úvodem do OSINT, kde se studenti seznámí s definicí, rozsahem a historickým kontextem OSINT. Studenti se naučí rozpoznávat a využívat jednotlivé typy otevřených zdrojů, jako jsou veřejné záznamy, webové stránky, sociální média a odborné publikace. Součástí je také hodnocení věrohodnosti, spolehlivosti a zkreslení zdrojů a techniky pro ověření zdrojů.

1. Co je to OSINT, kdo ho využívá a proč, jaké jsou jeho druhy.
2. Google dorking aneb googlování pro pokročilé.
3. Vyhledávání uživatelů a identit napříč internetem.
4. Získání informací a metadat z fotografií a dokumentů.
5. (Ne)zabezpečené kamery a IoT aneb stalkujeme na dálku.
6. Jak nepropadnout panice a zabezpečit sám sebe.

Kybermládež 101: Jak rozumět online světu vašich dětí (3-4h)

1. Úvod do světa kybermládeže
2. Proč je důležité rozumět jejich jazyku?
3. Historie a vývoj online komunikace mezi mládeží.
4. Nejčastější termíny a jejich významy
5. Představení Slovníku pro boomery.
6. Diskuse a ukázky z reálného života: jak a v jakém kontextu děti tyto termíny používají.
7. Trendy v online komunikaci
8. Populární sociální sítě a platformy, které děti momentálně používají.
9. Bezpečnost dětí na internetu
10. Nebezpečí a pasti online komunikace.
11. Sociální sítě a jejich nebezpečí.
12. Gaming, youtubeři a influenceři
13. Porno, OnlyFans, sexting a vydírání
14. Tipy na nástroje a aplikace pro sledování a omezení online aktivity dětí.
15. Jak komunikovat s dětmi o jejich online životě.

Používáme AI bezpečně (3-4h)

1. Historie a mechanismy
2. Typy neuronových sítí a generativních LLM
3. Jak používat AI a neohrozit firemní bezpečnost
4. Jak používají útočníci AI proti nám
5. Deepfake, jak ho udělat a jak ho poznat
6. Praktické ukázky
7. Lokální AI modely
8. Legislativa a autorská práva

Základy etického hackingu (16h)

(2 dny, celé, praktický workshop pro cca 4–10 účastníků ve virtuálním prostředí labů MS Azure)

Den 1 – Jak se dostat do firmy:

1. Úvod – Seznámení s prostředím laboratoří a Kali Linuxem
2. Mitre Att&ck prakticky
3. Recon – Shodan, Censys, DnsDumpster, Mxtoolbox…
4. OSINT – Maltego, Google dorking, metadata exfiltrace, Userrecon, Hunter.io
5. Sociální inženýrství – phishing prakticky, metody a triky útočníků, vishing, quishing, smishing
6. Fyzický redteaming – Picoducky, OM.G cable, Flipper zero, baiting – demonstrace reálných útoků
7. Skenování portů – nmap, Advanced IP Scanner, netcat, bannery
8. Získání přístupu – exploitace prakticky, tvorba generovaného malware, ovládnutí vzdáleného PC

Den 2 – Jdeme si pro doménového admina:

1. Úvod do Active Directory attack kill chain
2. Enumerace a recon
3. Local privilege escalation
4. Lateral Movement
5. Domain Privilege Escalation
6. Domain persistence

Možnost konzultace s vašimi reáliemi, doporučení praktických opatření.

Den 1. školí Pavel Matějíček – CEH, evangelista IT bezpečnosti, ex ESET, purple teamer, přednášející na Cyber Days 2022

Den 2. Lubomír Ošmera – lektor v Gopasu, Microsoft Security trainer, consultant and red teamer, přednášející na HackerFestu 2023