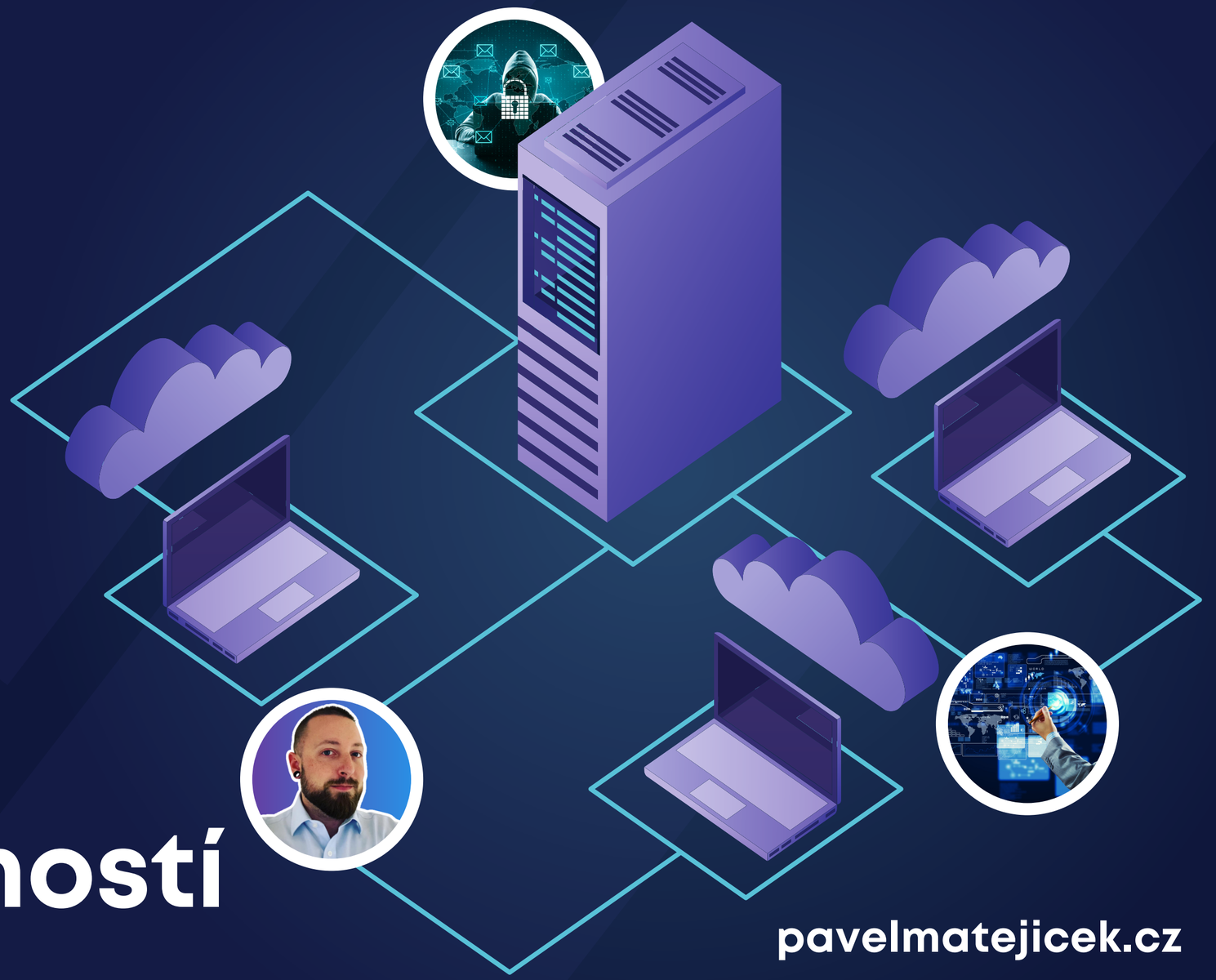
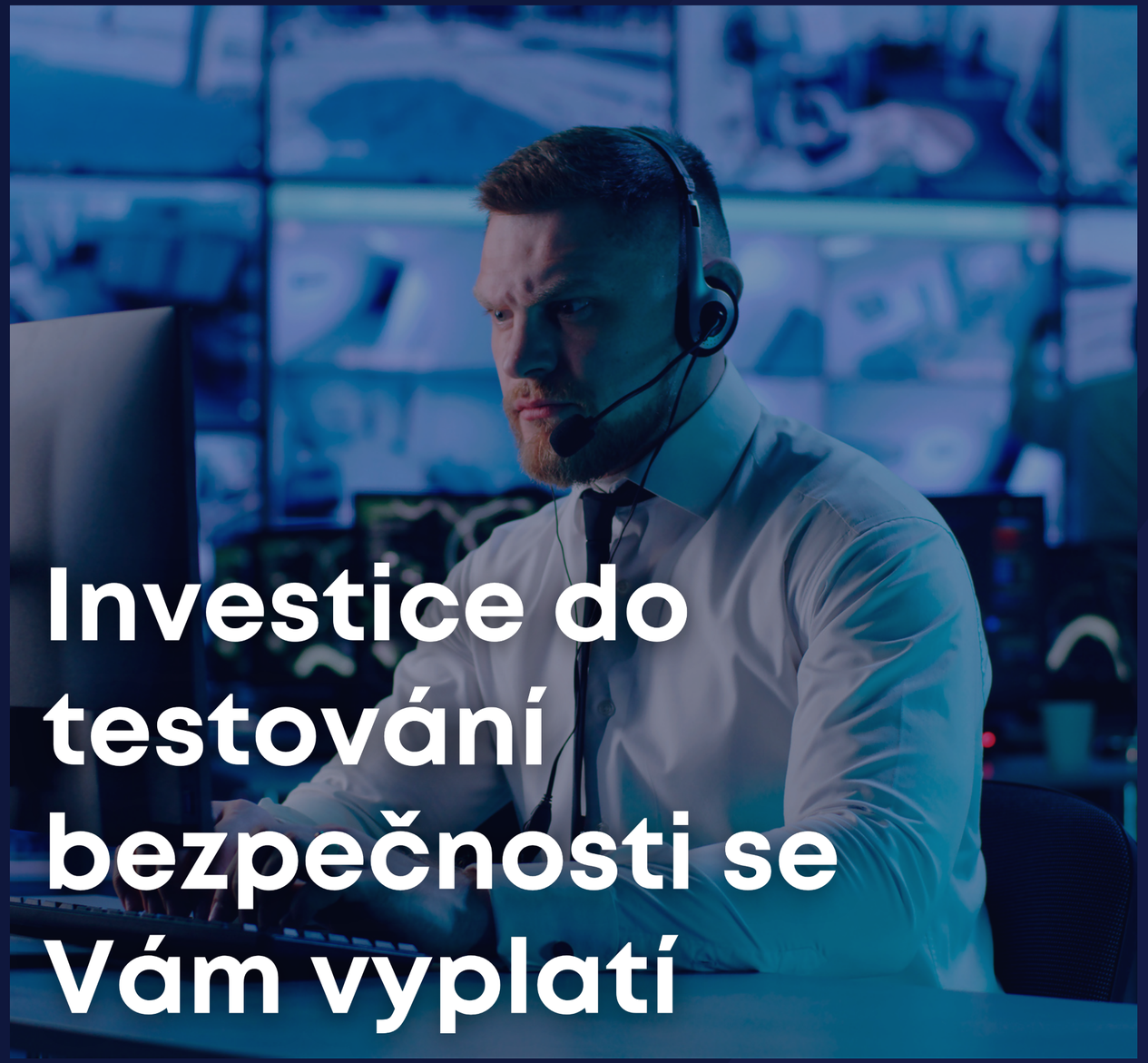
Pavel Matějíček

Sociální inženýrství
Testy zranitelností



pavelmatejicek.cz



Investice do testování bezpečnosti se Vám vyplatí

+83 %

společností není připraveno nést finanční dopady úspěšného útoku

+65 %

za většinou úspěšných hacknutí stál phishingový e-mail

1 až 5

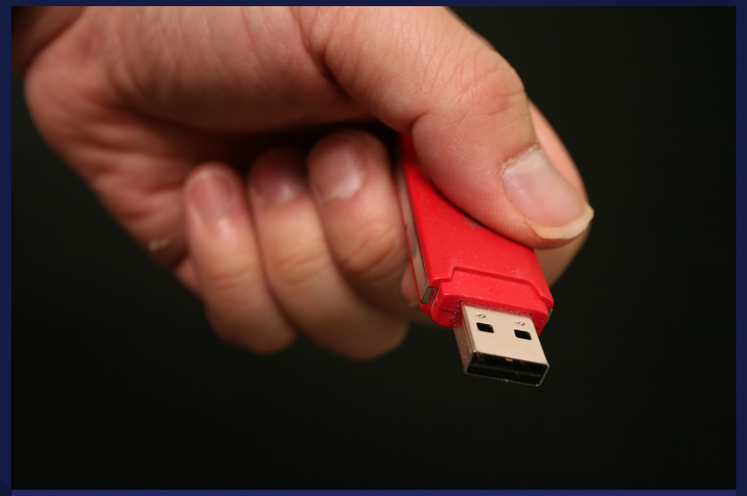
hesel používají Vaši zaměstnanci pro přihlašování k různým účtům

Sociální inženýrství

Phishingové testy

Podvodné e-maily které otestují připravenost zaměstnanců na reálný phishingový útok.

náchylnost zaměstnanců



Baiting

Co udělá zaměstnanec, když najde na zemi USB disk s citlivými daty?

náchylnost zaměstnanců

Vishing

Podvodné telefonáty, které mají za cíl vylákat ze zaměstnanců důvěrné informace.

náchylnost zaměstnanců

Sociální inženýrství

Phishingové testy

Test spočívá v tom, že pošlu várku podvržených e-mailových zpráv tak, aby vypadaly, že jsou to zprávy pravé.

Může se jednat o lákavou nabídku produktu, firemní benefity nebo e-mail, který se tváří jako od interního IT a vyzývá uživatele k nějaké akci.
Scénářů mám v zásobě mnoho.

Baiting

Jedná se o techniku sociálního inženýrství, kdy necháme zaměstnance zakousnout se do určité návnady – v tomto případě USB disku, který se nachází v blízkosti pracoviště.

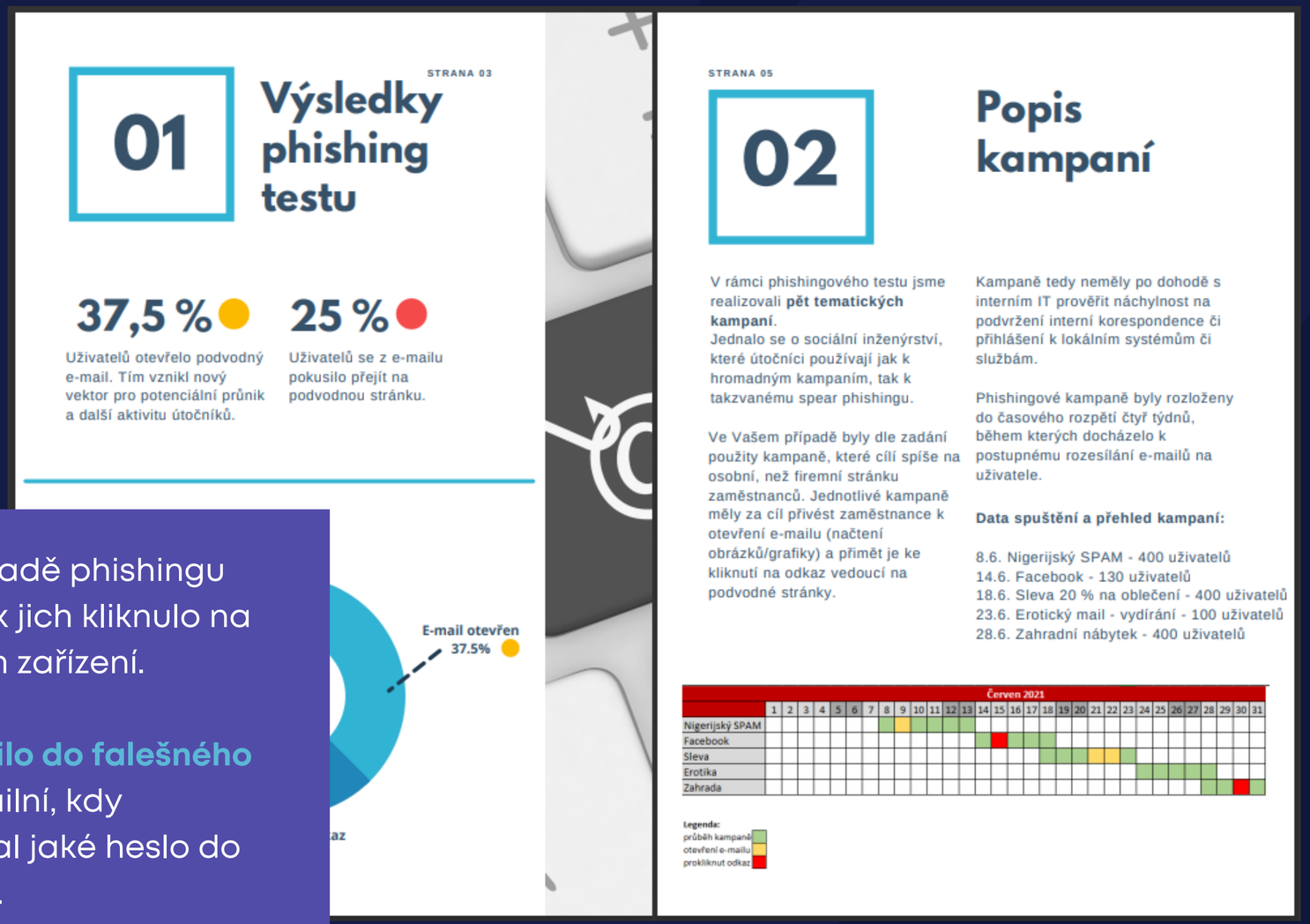
Pokud by se na tomto disku nacházel malware, došlo by ke kompromitaci společnosti.

Vishing

Pomocí podvodných telefonátů se specialisté pokusí ze zaměstnanců vytěžit citlivé informace, které by útočníci mohli použít k přípravě útoku a dalších kroků.

Jedná se obdobu mysteryshoppingu, zde se ale hraje o citlivá data.

Sociální inženýrství - vyhodnocení



STRANA 03

01 Výsledky phishing testu

37,5 % Uživatelů otevřelo podvodný e-mail. Tím vznikl nový vektor pro potenciální průnik a další aktivitu útočníků.

25 % Uživatelů se z e-mailu pokusilo přejít na podvodnou stránku.

E-mail otevřen 37.5%

STRANA 05

02 Popis kampaní

V rámci phishingového testu jsme realizovali **pět tematických kampaní**.
Jednalo se o sociální inženýrství, které útočníci používají jak k hromadným kampaním, tak k takzvanému spear phishingu.

Ve Vašem případě byly dle zadání použity kampaně, které cílí spíše na osobní, než firemní stránku zaměstnanců. Jednotlivé kampaně měly za cíl přivést zaměstnance k otevření e-mailu (načtení obrázků/grafiky) a přimět je ke kliknutí na odkaz vedoucí na podvodné stránky.

Kampaně tedy neměly po dohodě s interním IT prověřit náchylnost na podvržení interní korespondence či přihlášení k lokálním systémům či službám.

Phishingové kampaně byly rozloženy do časového rozpětí čtyř týdnů, během kterých docházelo k postupnému rozesílání e-mailů na uživatele.

Data spuštění a přehled kampaní:

8.6. Nigerijský SPAM - 400 uživatelů
14.6. Facebook - 130 uživatelů
18.6. Sleva 20 % na oblečení - 400 uživatelů
23.6. Erotický mail - vydírání - 100 uživatelů
28.6. Zahradní nábytek - 400 uživatelů

Červen 2021

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Nigerijský SPAM																															
Facebook																															
Sleva																															
Erotika																															
Zahrada																															

Legenda:
průběh kampaně
otevření e-mailu
prokliknut odkaz

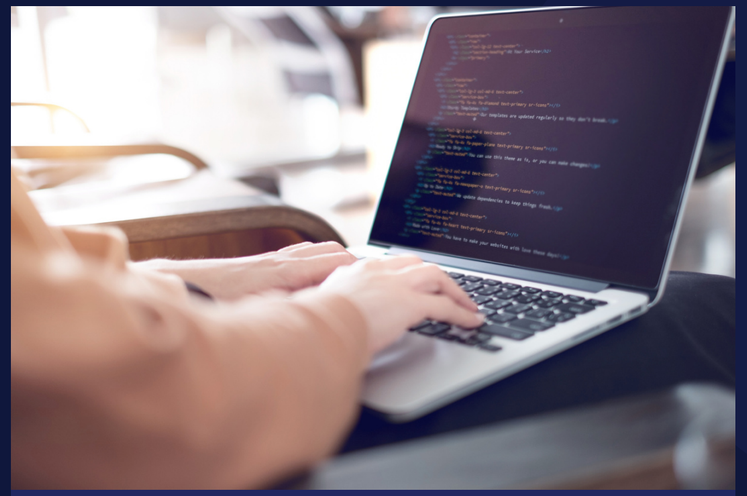
Měřím, jak byly kampaně úspěšné – v případě phishingu zjistím, kolik uživatelů zprávu otevřelo, kolik jich kliknulo na podvodný odkaz, v kolik hodin a na kterém zařízení.

Také uvidím, **kolik zaměstnanců se přihlásilo do falešného portálu.** Vyhodnocení může být velmi detailní, kdy uvidíme, který uživatel, na jaké pozici, zadal jaké heslo do kompromitovaného systému, kdy a odkud.

V případě USB disků **vidím, z jaké IP adresy došlo k otevření** kterého dokumentu a jsem notifikován e-mailem.

Všechna data zpracuji do závěrečné zprávy, kterou Vám i managementu rád osobně odprezentuji.

Testy zranitelností



Test bezpečnosti webů

Oskenuji Vaše webové stánky a zjistím zda jsou zranitelné či neprozrazují citlivá data.

míra ochrany

Aktivní sken infrastruktury

Otestuji porty a na nich běžící služby na známé zranitelnosti a exploity.

míra ochrany

Kontinuální monitoring

Budu monitorovat a pravidelně kontrolovat dostupnost a bezpečnost Vaší firmy.

míra ochrany

Testy zranitelností

Aktivní sken infrastruktury

- Kontrola otevřených portů
- Analýza běžících služeb
- Scan operačních systémů na výskyt exploitů
- Testování proti známým zranitelnostem (CVE)
- Vyhledávání subdomén a návazností na další služby
- Testování výchozích loginů
- Skenování interní sítě díky VPN profilu

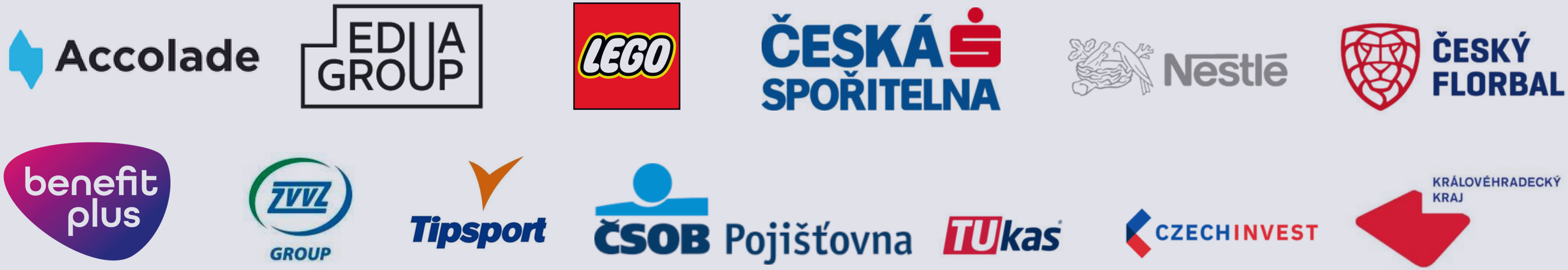
Test bezpečnosti webu

- Správná konfigurace HTTPS
- Bezpečné nastavení cookies
- Náchylnost na cross-site-scripting (XSS)
- Náchylnost na SQL injection
- Aktuálnost použitých technologií (JavaScript, PHP…)
- Test webserveru
- Ověříme zda na vašem webu nejsou dohledatelné citlivé dokumenty

Kontinuální monitoring

- Monitoring dostupnosti služeb podle portu či na ping 24/7/365
- Hlídání platnosti HTTPS certifikátů a včasné upozornění na expiraci
- Zjistíme, zda se hesla Vašich zaměstnanců neobjevila v uniklých databázích
- Pravidelný vulenrability scan – týdně, měsíčně, či kvartálně

Důvěřují mi společnosti všech typů a velikostí



Jak probíhá spolupráce?

Kontaktujte mě

Zjistím co potřebujete a upravím službu Vašim potřebám a možnostem

On-line schůzka

Domluvíme si datum realizace a vyřešíme technikálie

Objednávka

Domluvenou službu závazně objednáte, já ji dodám a pošlu fakturu

Kontaktujte mě

E-mail
info@pavelmatejicek.cz

Telefon
+420 702 029 676

Web
pavelmatejicek.cz