CyberCheck 360°

CyberCheck 360° je váš první a nejdůležitější krok k posílení kybernetické bezpečnosti – rychle a s maximálním přehledem. Tento vstupní balíček pokrývá tři klíčové oblasti, které rozhodují o vaší obranyschopnosti: prověříme technickou infrastrukturu pomocí penetračního testování, otestujeme připravenost zaměstnanců pomocí realistických phishingových kampaní a zkontrolujeme nastavení dokumentace a bezpečnostních procesů v souladu s požadavky NIS2. Za pár týdnů získáte jasnou a komplexní mapu rizik, silných i slabých míst – a konkrétní doporučení, kde začít budovat skutečně odolnou organizaci.

4CYBER

Balíček obsahuje:

1. GAP analýza kybernetické bezpečnosti (NIS2 Compliance Assessment)

Gap analýza kybernetické bezpečnosti je systematické zhodnocení aktuálního stavu ochrany vaší organizace ve srovnání s požadavky směrnice NIS2 a osvědčenými bezpečnostními standardy. Cílem je identifikovat nedostatky, slabá místa a oblasti, kde vaše systémy, procesy a pravidla neodpovídají požadované úrovni ochrany. Výsledkem analýzy je přehledný soupis rizik a prioritizovaný plán nápravných opatření, který vám umožní cíleně posílit vaši kybernetickou odolnost a připravit se na legislativní i reálné hrozby.

2. Penetrační testování IT infastruktury (Penetration Testing)

Penetrační testování IT infrastruktury je kontrolovaný simulovaný útok na vaše servery, sítě, systémy a aplikace, jehož cílem je odhalit technické zranitelnosti dříve, než je mohou zneužít skuteční útočníci. Testování zahrnuje analýzu zabezpečení z pohledu externího i interního útočníka a poskytuje detailní přehled o slabinách, jejich kritičnosti a možných scénářích zneužití. Výstupem je technická zpráva s konkrétními doporučeními na odstranění zranitelností a posílení celkové bezpečnosti vaší IT infrastruktury.

3. Phishingové testování zaměstnanců (Phishing Simulation)

Phishingové testování zaměstnanců je cílená simulace reálných phishingových útoků, jejímž cílem je ověřit odolnost lidí jako nejčastějšího slabého článku kybernetické bezpečnosti. Prostřednictvím různých scénářů, například falešných e-mailů nebo podvržených webových stránek, se testuje, jak zaměstnanci reagují na pokusy o získání citlivých údajů či přístupu do interních systémů. Výsledkem je analytická zpráva s vyhodnocením úspěšnosti útoků a konkrétní doporučení pro školení a zvýšení bezpečnostního povědomí v organizaci.

Balíček je navržen tak, aby rychle a efektivně prověřil vaši IT infrastrukturu, připravenost zaměstnanců na kybernetické útoky a nastavení klíčových bezpečnostních procesů. Díky tomu získáte jasný přehled o aktuálních rizicích, snížíte pravděpodobnost úniku dat, připravíte se na splnění požadavků NIS2 a zvýšíte důvěru klientů i partnerů ve vaši organizaci.

4CYBER

Cenová kalkulace:

Balíček služeb	Rozsah	Cena
CyberCheck 360°	• GAP analýza kybernetické bezpečnosti • Penetrační testování infrastruktury • Phishingové testování zaměstnanců • Závěrečné zprávy, manažerské shrnutí a reporty	**149 000,- Kč**

Rozsah služeb

Gap analýza kybernetické bezpečnosti dle NIS2

- Posouzení souladu aktuálních bezpečnostních opatření s požadavky směrnice NIS2
- Zhodnocení dokumentace, procesů řízení rizik a incidentů, řízení přístupů, BCM a školení
- Identifikace nesouladů a slabin
- Výstup: Podrobná zpráva s prioritizovaným plánem nápravných opatření

Penetrační testování IT infrastruktury

- Externí testování veřejně dostupných systémů (např. firewally, servery, VPN, weby)
- Testy základních síťových a aplikačních zranitelností
- 1 den vzdáleného testování (s technickou koordinací)
- Výstup: Technická zpráva s nálezy, mírou rizika a návrhem řešení

Phishingové testování zaměstnanců

- Jedna realistická phishingová kampaň pro až **250 zaměstnanců**
- Simulovaný útok e-mailem (různé scénáře – interní IT, banka, změna hesla atd.)
- Sledování míry kliknutí, zadání údajů a otevření příloh
- Výstup: Přehledné statistiky + doporučení pro školení a zvýšení povědomí

Závěrečná zpráva & konzultace

- Manažerské shrnutí výsledků (Executive Summary)
- Souhrnná závěrečná prezentace s doporučením dalšího postupu
- 1 online schůzka k interpretaci výstupů a návrhům opatření