ANALÝZA KYBERNETICKÉ BEZPEČNOSTI

Služby poskytované v rámci analýzy

- ZÁKLADNÍ ANALÝZA
- GAP ANALÝZA
- ANALÝZA RIZIK
- SKENOVÁNI ZRANITELNOSTÍ
- PENETRAČNÍ TEST – PERIMETR
- PENETRAČNÍ TEST – WIFI
- PENETRAČNÍ TEST – WEBOVÁ APLIKACE/PORTÁL
- POKROČILÁ ANALÝZA PROVOZU SE ZAMĚŘENÍM NA MALWARE

ZÁKLADNÍ ANALÝZA STAVU KYBERNETICKÉ BEZPEČNOSTI

POPIS SLUŽBY

Základní služba sloužící ke zjištění skutečného stavu informační a kybernetické bezpečnost z pohledu ISMS a z cílem určení kvality procesů, bezpečnostních nástrojů a řídící dokumentace. Služba vychází z kritérií dle metodiky CIS v8. Služba probíhá formou jednoduchého interview s předpokladem vyplnění jednoduchého dotazníku, který obsahuje jednotlivé oblasti.

VÝSTUPY

Situační mapa popisující stav informační a kybernetické bezpečnosti z pohledu:

- řídících procesů,
- řídící dokumentace,
- úrovně plnění legislativy,
- úrovně plnění dle programů kvality řízení,
- úrovně plnění požadavků regulace,
- stavu bezpečnosti (Informační fyzické, personální).

Namapování na základní score dle CIS v8

GAP ANALÝZA

POPIS SLUŽBY

Jedná se o analýzu současného stavu kybernetické bezpečnosti. Šetření probíhá formou analýzy interních dokumentů (směrnic), nástrojů, procesů, a analýzou a zpracováním vyplněných hodnot v zaslaných šablonách a řízenými online rozhovory s pracovníky společnosti a IT specialistu. (Osobní nebo Teams schůzky). GAP analýza je provedeny na základě standardů CIS v8 a na Základě standardů ISO 27001, NIST a požadavků ZoKB, případně NIS 2.0 (Dosud není zohledněna v ZoKB), GDPR nebo TISAX. Výstupem GAP Analýzy současného stavu kybernetické bezpečnosti je Závěrečná zpráva, která předkládá náhled ve čtyřech perspektivách, jejichž popis reprezentuje hlavní cíle provedené analýzy.

VÝSTUPY

- Současný stav – zahrnuje zhodnocení Strategie bezpečnosti ICT, Technologické zajištění kybernetické bezpečnosti, Procesní a organizační zajištění kybernetické bezpečnosti a Provozní úroveň zajištění kybernetické bezpečnosti.
- Cílový stav – na základě zjištění současného stavu, seznámení se s obchodními cíli organizace a řízeným pohovorem s představiteli vedení společnosti jsou stanoveny priority Strategie bezpečnosti organizace.
- Diferenční analýza – definice a popis konkrétních opatření, které je nezbytné realizovat pro dosažení cílového stavu kybernetické bezpečnosti organizace. Obsahuje score dle CIS v8
- Mapa projektů – časového vymezení realizace konkrétních IT projektů vymezených v Dif. analýze.

ANALÝZA RIZIK

POPIS SLUŽBY

Jedná se o analýzu bezpečnosti informačních aktiv současného stavu kybernetické bezpečnosti. Šetření probíhá formou analýzy interních dokumentů (směrnic), nástrojů, procesů, a analýzou a zpracováním vyplněných hodnot v zaslaných šablonách a řízenými onsite nebo online rozhovory s pracovníky společnosti a IT specialistu.

Metodika pro Analýzu rizik (AR) je postavena na základech požadavků ISO/IEC 27001 a zákona o kybernetické bezpečnosti a vychází, z identifikace aktiv (Z tohoto pohledu Informační systém a proces) a stanovení jejich důležitosti (Důvěrnosti/Dostupnosti a Integrity v rozsahu bodů 1-4). Z identifikace aktiv a stanovení míry úrovně (v úrovních 1-4/ Nízká, Střední, Vysoká/Kritická), tzn.

Hrozby (Pokud pro dané aktiva existuje), Zranitelnosti (Pokud pro dané aktiva existuje), Dopadu (Míra dopadu pro daná aktiva).

VÝSTUPY

- Komplexní správa o analýze rizik včetně BIA (Business Impact Analyze) a zmapování míry naplnění požadavků ISO/IEC 27001 s přihlédnutím k ISO/IEC 27002 a 27005 formou SOA, tzn analýzou aplikovatelnosti požadavků v prostředí subjektu a nebo pro prostředí dodavatelského řetězce.
- Výstupy BIA zohledňují finanční dopady v případě výpadku a nedostupnosti Procesu/-Služby v závislosti na informačním systému.

SKENOVÁNI ZRANITELNOSTÍ

POPIS SLUŽBY

Služba CRA Skenování zranitelností zahrnuje externí skenování známých zranitleností, tzn. skenování aktiv účastníka, které jsou dostupné z internetu. Skenovací scénáře služby obsahují výběr aktiv, typy skenů, interval skenování a další informace důležité pro provádění. Rozsah skenování je předem definován při přípravě skenovacích scénářů. Seznam testovaných známých zranitelností je pravidelně aktualizován. Pro skenování zranitelností je používán nástroj Nessus, který je ve vlastnictví ČRA.

VÝSTUPY

- Výstupem služby je identifikace známých zranitelnosti a doporučení, jak zjištěné zranitelnosti řešit.
- V rámci životního cyklu služby pracovní tým předává informace o zranitelnostech, které byly zjištěny. Vypořádání nápravy nálezů realizují odborné týmy na straně zákazníka, nebo partnerská společnost ČRA, pokud je správa systémů součástí poskytovaných služeb ČRA.
- V procesu poskytované služby je také řešena situace, kdy není možné danou zranitelnost odstranita je nutné ji řešit nadřazeným prvkem (Firewall, IPS).
- Zákazník obdrží podrobný report

PENETRAČNÍ TEST – PERIMETR

POPIS SLUŽBY

Jedná se o vnější bezpečnostní test perimetru, který představuje komplexní simulaci napadení síťových komponent útočníkem z vnějšího prostředí. Cílem je zjistit jak snadno identifikovatelný Cíl tato infrastruktura síťových komponent představuje, a jaké informace lze získat z venku (informace o dostupných komponentách a jejich zranitelnostech), které mohou být následně zneužity pro získání neautorizovaného přístupu.

Tyto testy probíhají formou:

- Identifikace služeb a zranitelností,
- Získání přístupů a eskalace privilegií a ovládnutí cíle
- Monitoringu reakce na testy (analýza reakce ochranných nástrojů NTA/IDS/IPS apod.)

VÝSTUPY

Závěrečná zpráva o průběhu penetračních testů obsahující detailní popis nálezů a zranitelností (Manažerské shrnutí a technická zpráva):

- Cíle a rozsahy testů
- Stanovení stupnice a metodik hodnocení
- Detailní postup provedených testů
- Popis zjištění a zranitelností, včetně doporučení k odstranění
- Závěrečné zhodnocení provedeného testu a hodnocení aktuálně dosažené úrovně bezpečnosti dle CIS v8

PENETRAČNÍ TEST – WIFI

POPIS SLUŽBY

Jedná se o vnitřní bezpečnostní test Wifi technologií, který představuje komplexní simulaci napadení těchto síťových komponent útočníkem z vnějšího prostředí. Cílem je zjistit jak snadno identifikovatelný Cíl tato infrastruktura síťových Wifi komponent představuje, a jaké informace lze získat z venku (informace o dostupných komponentách a jejich zranitelnostech), které mohou být následně zneužity pro získání neautorizovaného přístupu.

Tyto testy probíhají formou:

- Identifikace služeb a zranitelností,
- Získání přístupů a eskalace privilegií a ovládnutí cíle

V rámci testování vycházíme z následujících metodik, OWASP, MSTG, Top Ten, ASVS, MASVS OSSTMM, PTEST, NIST, CIS, PCI-DSS, CVE, CVSS

VÝSTUPY

Závěrečná zpráva o průběhu penetračních testů obsahující detailní popis nálezů a zranitelností (Manažerské shrnutí a technická zpráva):

- Cíle a rozsahy testů
- Stanovení stupnice a metodik hodnocení
- Detailní postup provedených testů
- Popis zjištění a zranitelností, včetně doporučení k odstranění
- Závěrečné zhodnocení provedeného testu a hodnocení aktuálně dosažené úrovně bezpečnosti dle CIS v8

PENETRAČNÍ TEST – WEBOVÁ APLIKACE/PORTÁL

POPIS SLUŽBY

Jedná se o vnější nebo vnitřní bezpečnostní test aplikace, webové aplikace atd, který představuje komplexní simulaci napadení jejich komponent útočníkem z vnější, nebo vnitřního prostředí. Cílem je zjistit jak snadno identifikovatelný Cíl tato aplikační infrastruktura představuje, a jaké informace lze o ní získat zvenku, nebo zevnitř (informace o dostupných komponentách a jejich zranitelnostech), které mohou být následně zneužity pro získání neautorizovaného přístupu.

V rámci testování vycházíme z následujících metodik, OWASP, MSTG, Top Ten, ASVS, MASVS OSSTMM, PTEST, NIST, CIS, PCI-DSS, CVE, CVSS

VÝSTUPY

Závěrečná zpráva o průběhu penetračních testů obsahující detailní popis nálezů a zranitelností (Manažerské shrnutí a technická zpráva):

- Cíle a rozsahy testů
- Stanovení stupnice a metodik hodnocení
- Detailní postup provedených testů
- Popis zjištění a zranitelností, včetně doporučení k odstranění
- Závěrečné zhodnocení provedeného testu a hodnocení aktuálně dosažené úrovně bezpečnosti dle CIS v8

POKROČILÁ ANALÝZA PROVOZU SE ZAMĚŘENÍM NA MALWARE

POPIS SLUŽBY

Pokročilá analýza je realizována prostřednictvím nástrojů pro pokročilou analýzu síťového provozu, který prostřednictvím umělé inteligence a strojového učení identifikuje kybernetické hrozby a útoky, které ostatní technologie nezaznamenají. Cílem analýzy je prostřednictvím auditu síťového provozu ověřit stav IT infrastruktury organizace a doporučit opatření pro zvýšení bezpečnosti, a to především v oblastech (detekce neznámých a cílených útoků a hrozeb, detekce známých útoků a hrozeb, ověření s bezpečnostními zásadami a politikami, výkonnost sítě a aplikací, vizualizace sítě a forenzní analýza).

VÝSTUPY

Výstupem je auditní zpráva která:

- Identifikuje reálnou úroveň zabezpečení sítě a provozní spolehlivosti.
- Obsahuje popis identifikovaných bezpečnostních, provozních nebo výkonnostních incidentů vč. detailního popisu incidentu. rizika a doporučení pro nápravu.
- Popisuje stavu sítě s jednotkami relevantních událostí bez falešně pozitivních detekcí. Report obsahuje URL odkazy na události pro zpětné prohlédnutí, včetně seznamu zařízení, uživatelů, podsítí, kterých s identifikovaný nedostatek týká.