2024

Nabídka služeb

CYBER SECURITY JAKO SLUŽBA

CYBER TBD

Komplexní řešení pro vaši digitální bezpečnost

Jako firma se specializujeme na poskytování komplexních řešení v oblasti kybernetické bezpečnosti, které jsou v souladu s nejnovějšími směrnicemi a standardy. Naše služby zahrnují široké spektrum možností od základní podpory až po kompletní správu bezpečnostních systémů, přičemž všechny jsou poskytovány týmem zkušených techniků s letitou praxí. Tento přístup nám umožňuje efektivně reagovat na individuální potřeby našich klientů a zajišťovat nejvyšší úroveň ochrany pro jejich informační systémy a data.

Naše bezpečnostní služby

Vulnerability Management

NIS2 VYŽADOVÁNO
ISO27001 A.8.8 / A.8.19

Security Awarenes Training

NIS2 VYŽADOVÁNO
ISO27001 A.6.3

Password Management

NIS2 VYŽADOVÁNO
ISO27001 A.5.17

Log Management

NIS2 VYŽADOVÁNO
ISO27001 A.8.15

Penetration Testing

NIS2 VYŽADOVÁNO
ISO27001 A.8.8

Monitoring Service

NIS2 VYŽADOVÁNO
ISO27001 vícero

Microsoft Security

NIS2 DOPORUČENO
ISO27001 vícero

Cyber Consulting

NIS2 DOPORUČENO
ISO27001 vícero

Skybox Security

NIS2 DOPORUČENO
ISO27001 vícero

Cloud WAF a DDoS

NIS2 DOPORUČENO
ISO27001 A.8.21 / A.8.22

Cyber TBD

Naše firma poskytuje špičkové služby v oblasti kybernetické bezpečnosti, založené na bohatých zkušenostech a rozsáhlém know-how našeho profesionálního týmu. Jsme odborníci na komplexní bezpečnostní řešení pro firmy různých velikostí, od malých podniků až po velké korporace s desítkami tisíc zaměstnanců a zařízení. Mimo jiné naše zkušenosti sahají napříč mnoha klíčovými průmyslovými odvětvími, včetně kritické infrastruktury, zdravotnictví, bankovnictví a cestovního ruchu.

Zkratka TBD (To Be Done) zdůrazňuje, že práce na zajištění kybernetické bezpečnosti není nikdy skutečně dokončena, ale je to neustálý proces, který vyžaduje průběžné zlepšování a adaptaci. Tento přístup odráží naši filozofii, že bezpečnostní opatření musí být vždy aktuální a v kroku s nejnovějšími hrozbami a technologiemi.

V naší firmě tento přístup znamená nejen pravidelné aktualizace a inovace našich služeb a řešení, ale také neustálé vzdělávání a rozvoj našich odborníků, aby byli schopni čelit nejnovějším výzvám v oblasti kybernetické bezpečnosti. Závazek k TBD (To Be Done) je pro nás závazkem k excelenci, neustálému zlepšování a poskytování špičkové ochrany pro naše klienty.

cybertbd.com →

Důvody, proč si vybrat naši firmu:

- **Zkušený a certifikovaný tým:**
  Naši odborníci drží mezinárodně uznávané certifikace od předních autorit v oblasti kybernetické bezpečnosti, včetně CompTIA Security+, Microsoft (SC-900, MS-900), NUKIB - Manažer kybernetické bezpečnosti, Qualys, Skybox Security SCPS+, Tenable, Zabbix, First CVSS, Elasticsearch, Cisco, PaloAlto. Tato odbornost zajišťuje, že naše služby jsou na nejvyšší možné úrovni.

- **Prokázané zkušenosti v klíčových odvětvích:**
  Naše zkušenosti s prací pro kritickou infrastrukturu, zdravotnická centra a technologické lídry v cestovním ruchu nám umožňují poskytovat specializované a cílené řešení, která přesně vyhovují potřebám těchto odvětví.

- **Komplexní znalost legislativy:**
  Máme hluboké znalosti směrnice NIS2 a jejího aktuálního výkladu, což nám umožňuje pomoci našim klientům splnit všechny právní a regulační požadavky.

- **Flexibilita a přizpůsobivost:**
  Naše zkušenosti s přebíráním služeb a implementací nových technologií nám umožňují flexibilně reagovat na specifické potřeby klientů a zajistit hladký přechod a integraci nových řešení.

- **Mezinárodní působnost:**
  Díky naší schopnosti pracovat na mezinárodní úrovni a rozsáhlé sítě partnerů můžeme nabídnout služby tam, kde jsou potřeba, a to s lokálním porozuměním a podporou.

Reference

Naše společnost si za poměrně krátkou dobu vybudovala pevnou pozici na trhu digitální bezpečnosti. Naše portfolio zahrnuje významné společnosti napříč různými sektory, včetně financí, telekomunikací, zdravotnictví a průmyslu.

Důvěru v naše služby nám svěřily firmy, které denně chrání citlivá data tisíců zákazníků, a jejichž operace závisí na bezpečných a spolehlivých IT systémech.

Služby, které v současnosti poskytujeme jsou prověřeny nejen širokým spektrem klientů, ale také jejich dlouhodobou spokojeností a úspěšnými výsledky v oblasti prevence a řešení kybernetických útoků.

Spokojení klienti

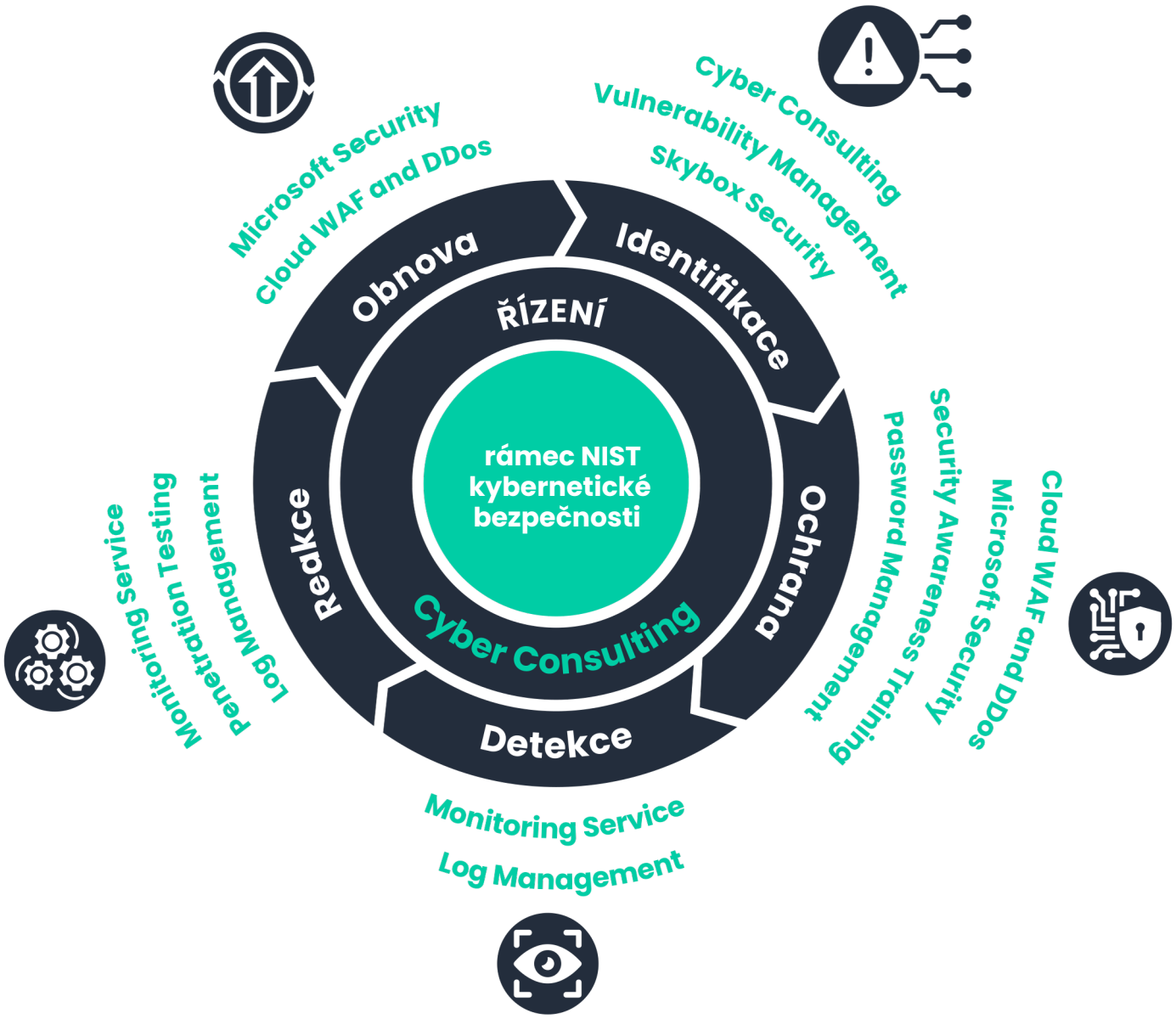
Vložte v nás svou důvěru →

Mapování NIS 2 s rámcem kybernetické bezpečnosti NIST

Směrnice NIS 2 stanovuje rozsáhlé povinnosti, ale neposkytuje konkrétní kroky. Přijetí rámce NIST (NIST Cybersecurity Framework) pomáhá organizacím účinně plnit požadavky NIS 2.

Rámec zahrnuje šest klíčových funkcí:

ŘÍZENÍ: Stanovení politiky pro efektivní řízení kybernetické bezpečnosti.
IDENTIFIKACE: Správa aktiv a hodnocení rizik.
OCHRANA: Ochrana sítě, přístupu a dat.
DETEKCE: Detekce incidentů a anomálií.
REAKCE: Plánování reakce na incidenty.
OBNOVA: Plánování obnovy a kontinuity provozu .



NIS2 VYŽADOVÁNO
ISO27001 A.8.8 / A.8.19

Vulnerability Management

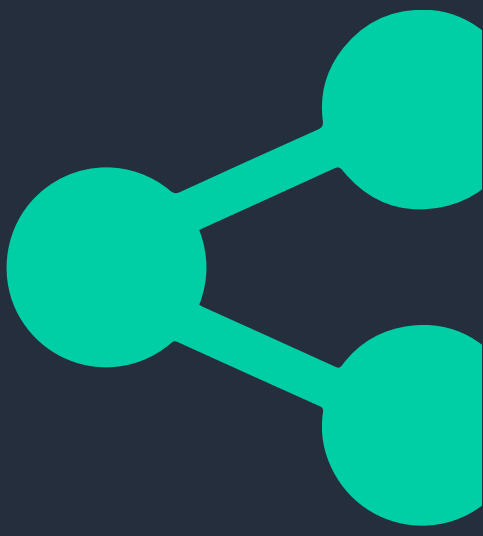
Služba správy zranitelností je zásadním prvkem v rámci kybernetického zabezpečení, poskytující organizacím klíčové nástroje pro identifikaci, analýzu a řízení zranitelností v jejich informačních systémech. Tato služba umožňuje organizacím **systematicky skenovat a vyhodnocovat zranitelné místa ve své infrastruktuře**, což je nezbytné pro efektivní ochranu proti kybernetickým útokům. Díky pravidelné identifikaci a analýze zranitelností mohou firmy proaktivně předcházet útokům, čímž minimalizují riziko úniku citlivých informací, finančních ztrát a poškození své reputace.

Jedním z hlavních benefitů služby správy zranitelností je, že pomáhá organizacím dodržovat nejrůznější předpisy a normy týkající se kybernetické bezpečnosti. Toto zahrnuje nařízení jako **GDPR**, **NIS**, **NIS2** a **PCI DSS**, které vyžadují od organizací zavedení a udržování adekvátních bezpečnostních opatření. Efektivní správa zranitelností zajišťuje, že organizace nejen splňují tyto normy, ale také se vyhnou potenciálně nákladným sankcím za jejich porušení.

Další klíčovou složkou této služby je **správa aktualizací a záplatování zranitelností**. Systematické zavádění bezpečnostních záplat a aktualizací je zásadní pro ochranu podnikových sítí a koncových zařízení před nově se objevujícími hrozbami. Tento proces nejenže zvyšuje celkovou kybernetickou odolnost organizace, ale také podporuje její důvěryhodnost a reputaci v očích klientů, partnerů a regulatorních orgánů.

Benefity služby

- **Proaktivní identifikace a řešení zranitelností**
- **Prevence úniku dat a finančních ztrát**
- **Dodržování regulatorních požadavků**
- **Zlepšení důvěryhodnosti a reputace**
- **Efektivní správa aktualizací a záplat**
- **Zvýšení celkové kybernetické odolnosti**



Objednat službu →

NIS2
ISO27001
VYŽADOVÁNO
A.6.3

Security Awarenes Training

Školení v kybernetické bezpečnosti jsou naprosto zásadní pro zajištění toho, že zaměstnanci jsou dobře informováni o neustále se měnících **bezpečnostních rizicích, legislativě a efektivních obranných strategiích**. V dnešní digitální době, kdy se kybernetické hrozby vyvíjejí neuvěřitelnou rychlostí, je pravidelná aktualizace znalostí a dovedností zaměstnanců nejen doporučena, ale přímo nezbytná. Naše školení poskytují zaměstnancům komplexní přehled o všech klíčových aspektech kybernetické bezpečnosti, který zahrnuje od základních principů po nejmodernější techniky obrany, umožňující jim nejen pochopit, ale i efektivně reagovat na potenciální hrozby.

Zaměstnanci jsou často označováni jako „první obranná linie“ v kybernetické bezpečnosti organizace.

Schopnost rozpoznat phishingový email, správně reagovat na podezřelé chování systému, nebo jednoduše správně používat a spravovat svá hesla může mít obrovský dopad na celkovou bezpečnost firmy. Bez dostatečného školení jsou zaměstnanci mnohem zranitelnější vůči útokům, což může vést k závažným bezpečnostním porušením s potenciálně devastujícími následky pro organizaci.

Školení v kybernetické bezpečnosti nejenže posiluje schopnosti zaměstnanců v oblasti rozpoznávání a reakce na kybernetické hrozby, ale také vytváří kulturu bezpečnosti ve firmě.

Benefity služby

- **Zvýšení povědomí o bezpečnostních rizicích**
- **Aktualizace znalostí o legislativě a standardních postupech**
- **Praktická aplikace poznatků**
- **Průběžné testování a hodnocení**
- **Zvýšení angažovanosti zaměstnanců**
- **Zlepšení interní bezpečnosti**

Objednat službu →

NIS2 VYŽADOVÁNO
ISO27001 A.5.17

Password Management

Správce hesel je klíčový nástroj pro moderní organizace, který **centralizuje ukládání, správu a zabezpečení hesel pro přístup k různým aplikacím a službám**. Tento systém nabízí klíčové výhody, jako jsou zabezpečení citlivých dat, jednoduchost použití, a možnosti auditů a sledování, což umožňuje organizacím udržet hesla v souladu s interními směrnicemi.

Hesla jsou automaticky generována a bezpečně uložena, což odstraňuje potřebu uživatelů pamatovat si mnoho různých hesel a zároveň snižuje riziko úniku dat a interních hrozeb.

Naše služba nabízí také **centrální správu a transparentnost**, která zjednodušuje auditování a sledování přístupových práv, zvyšuje produktivitu uživatelů a zajišťuje dodržování předpisů a bezpečnostních standardů. Díky těmto funkcím může vaše organizace efektivně řídit přístupové oprávnění a zabezpečit kritické informace proti neoprávněnému přístupu.

Náš zkušený tým vám pomůže s úspěšnou implementací správce hesel a zajistí důkladné proškolení vašich uživatelů, aby byli schopni systém efektivně využívat. S naší navazující službou získáte robustní řešení, které zvýší bezpečnost dat, usnadní auditování a sledování přístupů a zároveň zlepší celkovou produktivitu v rámci vaší organizace.

Benefity služby

- **Zabezpečení citlivých dat**
- **Centrální správa a transparentnost**
- **Jednoduchost použití**
- **Možnost auditů a sledování**
- **Dodržování předpisů a standardů**
- **Prevence úniku dat**
- **Snížení rizika interních hrozeb**
- **Zvýšená produktivita**

Objednat službu →

NIS2 VYŽADOVÁNO
ISO27001 A.12.4

Log Management

Naše služby v oblasti správy **logů a SIEM (Security Information and Event Management)** poskytují komplexní řešení pro **efektivní sběr, ukládání, analýzu a správu logových záznamů a bezpečnostních událostí z různých systémů a aplikací**. Tato integrace umožňuje organizacím centralizovat a systematizovat data z různých zdrojů do jediného úložiště, což značně usnadňuje monitorování, vyhodnocování a reagování na bezpečnostní incidenty.

Naši odborníci vyvíjejí **speciální parsery, konektory a kontrolní mechanismy**, které zajišťují, že jak log management, tak SIEM systémy poskytují maximální možnou hodnotu a efektivitu.

Díky našim službám mohou klienti, kteří již disponují těmito systémy, ale nevyužívají je k plnému potenciálu, získat značné zlepšení v oblasti reporting a analýzy dat. Pomáháme vytvářet užitečné případové studie, které demonstrují reálné výhody implementace a optimalizace SIEM systémů v praxi.

Naše služba je navržena tak, aby **transformovala velké objemy dat na smysluplné a stručné informace**, které poskytují užitečné náhledy pro rozhodování managementu. Cílem je zredukovat množství událostí, které vyžadují zásah, z tisíců na pouhé desítky nebo jednotky, což umožňuje rychlejší a přesnější reakce na skutečné hrozby a zlepšuje celkovou bezpečnostní situaci organizace. Tato efektivita nejen šetří čas, ale také značně snižuje náklady spojené s operativním zabezpečením IT prostředí.

Benefity služby

- **Centralizovaná správa dat**
- **Pokročilá analýza a reporting**
- **Optimalizace využití existujících systémů**
- **Efektivní reakce na hrozby**
- **Zlepšení rozhodování a plánování**
- **Snížení nákladů a zefektivnění procesů**
- **Dodržování předpisů**

Objednat službu →

NIS2 VYŽADOVÁNO
ISO27001 A.8.8

Penetration Testing

Naše služba **penetračního testování** nabízí důkladnou a **proaktivní kontrolu bezpečnosti vašich informačních systémů**. Na rozdíl od správy zranitelností, která se zaměřuje na identifikaci a opravu zranitelných míst v síti, penetrační testování aktivně simuluje skutečné útoky s cílem proniknout do vašich systémů. Tento přístup umožňuje našim zkušeným profesionálům nejen odhalit potenciální slabá místa, ale také posoudit, jak efektivně vaše aktuální bezpečnostní opatření dokáží čelit skutečným hrozbám.

Během penetračního testování naši odborníci systematicky prozkoumají vaše informační systémy, včetně aplikací a síťové infrastruktury, s cílem identifikovat jakékoli zranitelnosti, které by mohly být využity útočníky. **Proces zahrnuje řadu kontrolovaných útoků, které imitují aktivity kybernetických zločinců** a jsou zaměřeny na odhalení slabých míst, která by mohla být potenciálně zneužita.

Výsledkem těchto testů je detailní zpráva, která obsahuje **přehled identifikovaných zranitelností, hodnocení rizik spojených s každou z nich a doporučení pro posílení bezpečnostních opatření**. Tato zpráva poskytuje cenné informace, které vám pomohou přijmout potřebné kroky k zajištění vašich systémů a ochráně citlivých dat před skutečnými útoky.

Benefity služby

- **Odhalení a oprava zranitelností**
- **Simulace reálných kybernetických hrozeb**
- **Posílení bezpečnostních opatření**
- **Snížení rizika úniku dat a finančních ztrát**
- **Dodržování regulačních požadavků**
- **Zvýšení důvěry zákazníků a partnerů**

Objednat službu →

NIS2 VYŽADOVÁNO
ISO27001 vícero

Monitoring Service

Monitoring IT infrastruktury je nezbytný pro udržení nepřetržitého a efektivního provozu všech vašich systémů, serverů, sítí a aplikací. **Umožňuje sledovat stav a výkon infrastruktury v reálném čase**, identifikovat problémy ještě před jejich eskalací a okamžitě na ně reagovat. **Správně nastavený monitorovací systém zajišťuje efektivní řízení zdrojů, optimalizaci výkonu a minimalizaci rizika výpadků.**

Nasazení a správa takového systému vyžadují pokročilé odborné znalosti. Naše společnost se specializuje na poskytování komplexních služeb v oblasti monitoringu IT infrastruktury. Náš tým kvalifikovaných expertů s bohatými zkušenostmi vám pomůže s návrhem, implementací a správou monitorovacích řešení, aby **vaše infrastruktura fungovala bezchybně.**

Kromě toho zaškolíme vaše IT specialisty, aby plně využívali personalizované dashboardy a efektivně pracovali s triggerovanými událostmi. Tímto způsobem budou vaši experti schopni proaktivně reagovat na potenciální problémy ještě předtím, než ovlivní provoz, což **minimalizuje riziko výpadků a zajistí spolehlivý chod vašich systémů.**

Benefity služby

- **Profesionální nasazení monitorovacího systému**
- **Nepřetržitá správa a podpora**
- **Optimalizace výkonu**
- **Rychlé a efektivní řešení incidentů**
- **Proaktivita řešení**
- **Zlepšení rozhodování a plánování**
- **Dodržování regulačních požadavků**
- **Zvýšení důvěry zákazníků a partnerů**

Objednat službu →

NIS2
ISO27001

DOPORUČENO
vícero

Microsoft Security

Microsoft Security poskytuje komplexní odborné poradenství a podporu pro všechny aspekty prostředí **Microsoft 365**, od plánování a nasazení až po správu a optimalizaci. Specializujeme se na řízení implementace, kde naše ověřené postupy pomáhají optimalizovat konfiguraci systémů, aby se maximalizovalo využití Microsoft 365 a zvýšila návratnost investic.

Pro zajištění nejvyšší úrovně kybernetické bezpečnosti našim klientům nabízíme **integrované bezpečnostní řešení pomocí nástrojů jako Microsoft Defender a Azure Sentinel**. Tyto nástroje poskytují robustní ochranu proti široké škále kybernetických hrozeb a umožňují proaktivní sledování, detekci a reakci na bezpečnostní incidenty v reálném čase.

Důraz klade na implementaci **standardních operačních postupů (SOP) a dodržování branžových standardů**, což je klíčové pro zajištění souladu s nejlepšími praxemi a regulativními požadavky. SOP poskytují jasná pravidla a postupy, které standardizují operace zabezpečení a správy informací, což vede k zajištění konzistence a snížení rizik spojených s lidským faktorem.

Optimalizované bezpečnostní operace Microsoftu přinášejí významné přínosy organizacím, které využívají jejich technologie, tím, že neustále vylepšují své bezpečnostní funkce a mechanismy. Microsoft investuje do vývoje a aktualizací svých bezpečnostních nástrojů a služeb, aby zajistil, že jeho produkty a klienti jsou chráněni proti neustále se vyvíjejícím kybernetickým hrozbám.

Benefity služby

- **Maximalizace využití investic**
- **Proaktivní ochrana**
- **Rychlá reakce na incidenty**
- **Soulad s předpisy**
- **Zlepšení bezpečnostních operací**
- **Zvýšení důvěryhodnosti organizace**
- **Snížení operativních rizik**

Objednat službu →

NIS2
ISO27001

DOPORUČENO
vícero

Cyber Consulting

Naše služba **cyber consultingu** poskytuje organizacím specifické odborné poradenství a podporu v oblasti kybernetické bezpečnosti. Tento servis je navržen tak, aby **identifikoval, analyzoval a řešil bezpečnostní hrozby a rizika**, kterým organizace čelí. Specializujeme se na různé aspekty kybernetické bezpečnosti, včetně strategie, řízení rizik, implementace bezpečnostních technologií a incident response.

Outsourcing klíčových rolí, jako jsou **manažer kybernetické bezpečnosti (MKB)** a **architekt kybernetické bezpečnosti (AKB)**, organizacím umožňuje využívat odborné znalosti a zkušenosti našeho externího týmu bez nutnosti vynakládat zdroje na jejich interní zaměstnání a správu. Tím se **snižují náklady a zároveň zvyšuje účinnost a flexibilita v reakcích na bezpečnostní výzvy**.

Využitím našich konzultačních služeb získávají organizace **přístup k špičkovým odborníkům a metodám v oblasti kybernetické bezpečnosti**, což jim umožňuje zlepšit svou obranyschopnost, snížit rizika spojená s kybernetickými hrozbami a ochránit své informační systémy a data. Naše služby jsou navrženy tak, aby poskytovaly ucelené řešení kybernetické bezpečnosti přizpůsobené specifickým potřebám a cílům každé organizace.

Benefity služby

- **Přístup k odborným znalostem**
- **Snížení nákladů**
- **Zvýšení úrovně bezpečnosti**
- **Flexibilní a škálovatelné řešení**
- **Proaktivní řízení rizik**
- **Ochrana citlivých dat a systémů**
- **Dodržování legislativních a regulačních požadavků**

Objednat službu →

NIS2
ISO27001

DOPORUČENO
vícero

Skybox Security

Nasazení a správa **Skybox Security** vyžaduje odborné znalosti. Náš certifikovaný tým zajišťuje kompletní služby od nasazení a konfigurace, přes správu specifických modulů, až po plnou správu platformy. **Správný management Skyboxu** je klíčový pro optimální fungování všech jeho funkcí a maximální bezpečnostní přínosy.

Naše služby zahrnují:

- Nasazení a kompletní správa Skyboxu
- Podpora a konzultace
- Školení a vzdělávání
- Integrace do firemních procesů

Tím zajistíme **efektivní využití Skyboxu** ve vaší organizaci, což povede k výraznému zvýšení bezpečnosti a řízení rizik.

Skybox Security je pokročilá platforma pro správu kybernetické bezpečnosti, která pomáhá organizacím optimalizovat jejich bezpečnostní infrastrukturu. Díky integraci dat z různých bezpečnostních systémů poskytuje **Skybox kompletní pohled na celou síť** a identifikuje zranitelnosti, analyzuje rizika a podporuje strategické rozhodování v oblasti bezpečnosti. Platforma zahrnuje nástroje pro simulaci útoků, analýzu bezpečnostních politik, správu firewallů, a dynamickou mapu sítě, což umožňuje proaktivní ochranu před hrozbami.

Benefity služby

- **Kompletní nasazení a konfigurace Skyboxu**
- **Specializované projektové služby pro konkrétní moduly**
- **Důkladný management a pravidelná údržba platformy**
- **Maximální využití všech funkcionalit Skyboxu**
- **Snížení rizik v síťové infrastruktuře**
- **Optimalizace nákladů a zefektivnění procesů**

Objednat službu →

NIS2
ISO27001

DOPORUČENO
A.8.21 / A.8.22

Cloud WAF a DDoS

Naše služby **Cloud WAF (Web Application Firewall)** a **DDoS ochrana** jsou navrženy tak, aby poskytovaly **komplexní zabezpečení webových aplikací a sítí** proti široké škále kybernetických hrozeb.

Cloud WAF je robustní **bezpečnostní řešení umístěné v cloudu**, které chrání vaše webové aplikace před nebezpečnými útoky, včetně SQL injection, cross-site scripting (XSS), a dalšími typy zneužití zranitelností. Nabízí uživatelsky přívětivé rozhraní, které umožňuje snadno konfigurovat bezpečnostní pravidla, sledovat provoz a analyzovat bezpečnostní události v reálném čase. Toto řešení pomáhá včas identifikovat a řešit bezpečnostní hrozby, dříve než mohou způsobit škodu.

DDoS ochrana je zaměřena na **prevenci útoků typu DoS (Denial of Service) a DDoS (Distributed Denial of Service)**, které cílí na přetížení webových aplikací nebo sítí velkým množstvím požadavků, čímž je činí nedostupnými pro legitimní uživatele. Naše DDoS ochrana zahrnuje pokročilé detekční a filtrační technologie, které aktivně monitorují a mitigují potenciální útoky, udržujíce vaše služby dostupné i během velkých útočných kampaní.

Obě služby jsou navrženy s důrazem na snadnou správu a škálovatelnost, což umožňuje **přizpůsobení ochrany specifickým potřebám a velikosti vaší organizace**. Díky cloudovému řešení jsou naše služby rychle nasaditelné a nevyžadují složitou infrastrukturu ani vysoké počáteční investice, což činí naše bezpečnostní řešení ideální pro firmy všech velikostí, které chtějí chránit své online prostředky efektivně a ekonomicky.

Benefity služby

- **Komplexní ochrana**
- **Proaktivní bezpečnostní monitoring**
- **Uživatelsky přívětivé rozhraní pro snadné nastavení**
- **Škálovatelnost**
- **Prevence finančních ztrát**
- **Dodržování bezpečnostních standardů a předpisů**
- **Rychlá implementace**

Objednat službu →

CYBERTBD

cybertbd.com
sales@cybertbd.com
IČO: 21414432
DIČ: CZ21414432
D-U-N-S: 984089981