kybernetická bezpečnost,

Kybernetická bezpečnost je obor, který se zabývá ochranou počítačových sítí, hardware, software a dat před neoprávněným přístupem, zneužitím nebo poškozením. Cílem kybernetické bezpečnosti je chránit organizace a jednotlivce před útoky ze strany hackerů a zabránit zneužití počítačových sítí k nelegálním činnostem.

Kybernetická bezpečnost se týká širokého spektra počítačových sítí, včetně internetu, firemních počítačových sítí, sítí pro domácnosti a mobilních sítí. Kybernetická bezpečnost se zabývá ochranou před škodlivým softwarem, jako jsou viry a malware, a také ochranou před neoprávněným přístupem k počítačovým sítím a osobním údajům.

Pro zajištění kybernetické bezpečnosti jsou používány různé techniky, včetně firewally, šifrování dat, autentizace uživatelů a dalších opatření. Je důležité, aby organizace a jednotlivci pečlivě sledovali aktuální hrozby a pravidelně aktualizovali své bezpečnostní opatření, aby se vyhnuli útokům na své počítačové sítě.

kyberochrana

Kyberochrana je souhrnný termín pro opatření a techniky používané k ochraně počítačových sítí, hardware, software a dat před neoprávněným přístupem, zneužitím nebo poškozením. Kyberochrana zahrnuje široké spektrum aktivit, od preventivních opatření, jako je šifrování dat a autentizace uživatelů, až po reaktivní opatření, jako je odstraňování malware nebo obnova počítačových sítí po útoku.

Kyberochrana je důležitá pro ochranu osobních údajů, firemních tajemství a dalších cenných dat před útoky ze strany hackerů a nelegálními činnostmi. Je také důležitá pro zajištění spolehlivosti a důvěryhodnosti počítačových sítí a pro zachování integrity dat. Organizace a jednotlivci by se měli zabývat kyberochranou a pravidelně aktualizovat svá bezpečnostní opatření, aby se vyhnuli útokům a zajistili ochranu svých počítačových sítí a dat.

kyberprostor,

Kyberprostor je virtuální prostor, který je vytvářen pomocí počítačových sítí a technologií a který je používán pro komunikaci, výměnu informací a provádění různých činností. Kyberprostor zahrnuje internet a další počítačové sítě, včetně firemních počítačových sítí, sítí pro domácnosti a mobilních sítí.

Kyberprostor se liší od fyzického prostoru tím, že se v něm lidé a organizace mohou setkávat a komunikovat prostřednictvím počítačů a dalších zařízení připojených k počítačovým sítím, aniž by se museli fyzicky přesouvat z jednoho místa na druhé. Kyberprostor také umožňuje rychle a efektivně přenášet velké množství dat a informací po celém světě.

kyberkriminalita

Kyberkriminalita je označení pro trestné činy, které jsou spáchány prostřednictvím počítačových sítí nebo technologií. Kyberkriminalita zahrnuje široké spektrum činností, od nelegálního přístupu k počítačovým sítím přes krádež osobních údajů až po distribuci škodlivého software.

Kyberkriminalita může mít škodlivé důsledky pro jednotlivce i organizace, včetně finančních ztrát, poškození reputace a ztráty důvěry. Je důležité, aby organizace a jednotlivci chránili své počítačové sítě a osobní údaje pomocí různých opatření kybernetické bezpečnosti a byli si vědomi možných hrozeb kyberkriminality.

Incident/událost

Zákon č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)
(1) Kybernetickou bezpečnostní událostí je událost, která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací.

(2) Kybernetickým bezpečnostním incidentem je narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací v důsledku kybernetické bezpečnostní události.

(3) Orgány a osoby uvedené v § 3 písm. b) až e) jsou povinny detekovat kybernetické bezpečnostní události v jejich významné síti, informačním systému kritické informační infrastruktury, komunikačním systému kritické informační infrastruktury nebo významném informačním systému.

LEGISLATIVA

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)

Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (Směrnice NIS)

Vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích

Nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury

Vyhláška č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby

Vyhláška č. 316/2021 Sb., o některých požadavcích pro zápis do katalogu cloud computingu

Vyhláška č. 315/2021 Sb., o bezpečnostních úrovních pro využívání cloud computingu orgány veřejné moci

bezpečnostní management v oblasti kybernetiky

Bezpečnostní management v oblasti kybernetiky se zabývá plánováním, organizováním, řízením a kontrolou opatření zaměřených na ochranu počítačových sítí, hardware, software a dat před neoprávněným přístupem, zneužitím nebo poškozením. Cílem bezpečnostního managementu v oblasti kybernetiky je zajistit, aby organizace byla schopná ochránit své počítačové sítě a osobní údaje před útoky ze strany hackerů a nelegálními činnostmi a aby mohla spolehlivě a bezpečně využívat počítačové technologie.

Bezpečnostní management v oblasti kybernetiky zahrnuje široké spektrum aktivit, včetně identifikace hrozeb, hodnocení rizik, plánování bezpečnostních opatření, implementace a údržby bezpečnostních opatření a řízení incidentů bezpečnosti. Je důležité, aby organizace vyvinuly a implementovaly efektivní bezpečnostní strategii a procesy, které jim pomohou chránit své počítačové sítě a osobní údaje a zajistit spolehlivost a důvěryhodnost svých počítačových systémů.

Kybernetická bezpečnost v agendě státu?

Kybernetická bezpečnost je důležitou součástí agendy mnoha států, protože počítačové sítě a technologie jsou nyní klíčovým prvkem mnoha aspektů moderní společnosti a ekonomiky. Kybernetická bezpečnost se týká nejen ochrany počítačových sítí a dat před útoky ze strany hackerů a nelegálními činnostmi, ale také ochrany kritické infrastruktury, jako jsou například elektrická síť nebo vodovody.

Proto mnoho států zavádí různá opatření kybernetické bezpečnosti, aby ochránily své počítačové sítě a kritickou infrastrukturu před útoky a zajistily spolehlivost a důvěryhodnost svých počítačových systémů. Tyto opatření mohou zahrnovat vytvoření národních bezpečnostních strategií, zřízení bezpečnostních center nebo kybernetických jednotek, vzdělávání veřejnosti o bezpečnosti v kyberprostoru a spolupráci s mezinárodními partnery při řešení kybernetických hrozeb.

Jaké jsou vnější zranitelnosti kybernetické bezpečnosti?
LIDSKÝ FAKTOR
Vnější zranitelnosti kybernetické bezpečnosti jsou rizika a hrozby, které přicházejí ze vnějšku organizace a mohou ohrozit počítačové sítě a technologie. Mezi příklady vnějších zranitelností kybernetické bezpečnosti patří:

- Útoky ze strany hackerů: Útoky ze strany hackerů mohou představovat nebezpečí pro počítačové sítě a osobní údaje. Hackerské útoky mohou zahrnovat nelegální přístup k počítačovým sítím, krádež osobních údajů nebo distribuci škodlivého software.
- Útoky DDoS (Distributed Denial of Service): Útoky DDoS jsou útoky, při kterých je cílová počítačová síť nebo webová stránka zahlcena velkým množstvím požadavků, což ji činí nedostupnou pro oprávněné uživatele.
- Phishing: Phishing je typ útoku, při kterém útočník využívá podvodné e-maily nebo textové zprávy k získání osobních údajů nebo přístupových údajů od obětí.
- Malware: Malware je škodlivý software, který může poškodit počítačové sítě nebo osobní údaje. Malware může být distribuován prostřednictvím škodlivých e-mailů, škodlivých webových stránek nebo stažením škodlivého souboru.

Je důležité, aby organizace vyvíjely opatření kybernetické bezpečnosti, která jim pomohou chránit se před těmito vnějšími zranitelnostmi a zajistit spolehlivost a důvěryhodnost svých počítačových systémů.