Naše znalosti pro Váš úspěch

Nakladatelství **FORUM**

a

ACRESIA Consulting

Kybernetická bezpečnost – kontroly a sankce

Sankce dle NIS2

Čl. 36 - Členské státy stanoví sankce za porušení vnitrostátních opatření

Za stejné jednání pouze jedna sankce v souladu se zásadou zákazu dvojího trestání. Správní pokuty se ukládají spolu s kterýmkoli z opatření uvedených v čl. 32 odst. 4 písm. a) až h), čl. 32 odst. 5 a čl. 33 odst. 4 písm. a) až g)

Členské státy zajistí, aby správní pokuty ukládané základním a důležitým subjektům byly **účinné, přiměřené a odrazující**. Musí být Komisi oznámeny nejpozději do 17. ledna 2025.

Při rozhodování o uložení správní pokuty a při rozhodování o její výši se v každém jednotlivém případě náležitě přihlédne alespoň k prvkům uvedeným v čl. 32 odst. 7

Členské státy zajistí, aby v případě, že **základní** subjekty poruší článek 21 nebo 23, byly uvedeným subjektům v souladu s odstavci 2 a 3 tohoto článku uloženy správní pokuty, jejichž maximální výše bude stanovena na nejméně **10 000 000 EUR** nebo maximálně na alespoň **2 % celkového celosvětového ročního obratu** v předchozím rozpočtovém roce u podniku, ke kterému patří základní subjekt, podle toho, co je vyšší.

Členské státy zajistí, aby v případě, že **důležité** subjekty poruší článek 21 nebo 23, byly uvedeným subjektům v souladu s odstavci 2 a 3 tohoto článku uloženy správní pokuty, jejichž maximální výše bude stanovena na nejméně **7 000 000 EUR** nebo maximálně na alespoň **1,4 % celkového celosvětového ročního obratu** v předchozím rozpočtovém roce u podniku, ke kterému patří základní subjekt, podle toho, co je vyšší.

Hlava VI ZoKB

Kontrola vykonávaná Úřadem

Naše znalosti pro Váš úspěch

Úřad vykonává kontrolu v oblasti kybernetické bezpečnosti. Při výkonu kontroly Úřad zjišťuje, **jak orgány a osoby plní povinnosti** stanovené tímto zákonem, rozhodnutími a opatřeními obecné povahy vydanými Úřadem podle tohoto zákona, **a dodržují vyhlášky Úřadu**.

Při výkonu kontroly se postupuje podle kontrolního řádu.
CELEX 32022L2555

Zjistí-li Úřad, že orgán nebo osoba neplní povinnosti stanovené tímto zákonem nebo na základě tohoto zákona, **může uložit** orgánu nebo osobě, **aby zjištěné nedostatky ve stanovené lhůtě odstranila**, popřípadě **určit jakým způsobem**.

NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

Hlava VI ZoKB

Přestupky

Naše znalosti pro Váš úspěch

Vyšší povinnosti

- **neprovede registraci** nebo změnu registrace
- nenahlásí registrační a kontaktní údaje nebo další údaje nebo jejich změnu Úřadu
- nezajišťuje dostatečnou **zastupitelnost fyzických osob** oprávněných jednat
- při stanovení rozsahu řízení kybernetické bezpečnosti neidentifikuje všechna **primární aktiva** nebo **jejich identifikaci pravidelně nepřezkoumává** nebo neaktualizuje
- při stanovení rozsahu řízení kybernetické bezpečnosti **neurčí všechna primární aktiva** související s poskytováním regulované služby nebo organizační části a podpůrná aktiva podle nebo jejich určení **pravidelně nepřezkoumává nebo neaktualizuje**
- nevede **dokumentovaný záznam o identifikaci** a určení organizačních částí a aktiv
- **nezavede nebo neprovádí bezpečnostní opatření**
- **neohlásí kybernetický bezpečnostní incident** nebo nepředloží prvotní hlášení o incidentu anebo nedoplní některý z údajů o incidentu
- **neposkytne informace nebo součinnost** při zvládání incidentu
- neplní povinnost informovat uživatele regulované služby o kybernetickém bezpečnostním incidentu s významným dopadem
- neplní povinnost informovat uživatele regulované služby o významné hrozbě a krocích, které může uživatel služby učinit v reakci na ni
- neoznámí provedení protiopatření uložené Úřadem a jeho výsledek
- neplní povinnost uloženou Úřadem rozhodnutím o výstraze
- neplní povinnost uloženou rozhodnutím o vydání reaktivního protiopatření nebo opatřením obecné povahy vydaným Úřadem
- **nezohlední požadavky vyplývající z bezpečnostních opatření při výběru dodavatele** nebo ve smlouvě s dodavatelem
- neplní některou z povinností uloženou rozhodnutím o uložení nápravného opatření

Nižší povinnosti

- neprovede registraci nebo změnu registrace
- nenahlásí registrační, kontaktní údaje nebo další údaje nebo jejich změnu Úřadu nezajišťuje dostatečnou zastupitelnost fyzických osob oprávněných jednat
- při stanovení rozsahu řízení kybernetické bezpečnosti neidentifikuje všechna primární aktiva nebo jejich identifikaci pravidelně nepřezkoumává nebo neaktualizuje
- při stanovení rozsahu řízení kybernetické bezpečnosti neurčí všechna primární aktiva související s poskytováním regulované služby nebo organizační části a podpůrná aktiva, nebo jejich určení pravidelně nepřezkoumává nebo neaktualizuje
- nevede dokumentovaný záznam o identifikaci a určení organizačních částí a aktiv nezavede nebo neprovádí bezpečnostní opatření
- neohlásí kybernetický bezpečnostní incident nebo nepředloží prvotní hlášení o incidentu nebo nedoplní některý z údajů o incidentu
- neposkytne informace nebo součinnost při zvládání incidentu
- neplní povinnost informovat uživatele regulované služby o kybernetickém bezpečnostním incidentu s významným dopadem
- neplní povinnost informovat uživatele regulované služby o významné hrozbě a krocích, které může uživatel služby učinit v reakci na ni
- neoznámí provedení protiopatření uložené Úřadem a jeho výsledek
- neplní povinnost uloženou Úřadem rozhodnutím o výstraze
- neplní povinnost uloženou rozhodnutím o vydání reaktivního protiopatření nebo opatřením obecné povahy vydaným Úřadem
- nezohlední požadavky vyplývající z bezpečnostních opatření při výběru dodavatele nebo ve smlouvě s dodavatelem
- neplní některou z povinností uloženou rozhodnutím o uložení nápravného opatření

ID Rizika	Aktivum	Zranitelnost	Úroveň zranitelnosti	Hrozba	Úroveň hrozby	Úroveň dopadu	Z_Nr	H_Nr	D_Nr	Index rizika	úroveň rizika	Název rizika
1	Cloudová infrastruktura	nedostatečná údržba informačního a komunikačníh	Nízká	škodlivý kód (například viry, spyware, trojské koně),	Nízká	Vysoký	1	1	3	3	1	Napadení Ransomwarem
2	Cloudová infrastruktura	nedostatečná údržba informačního a komunikačníh	Nízká	poškození nebo selhání technického anebo programového vybavení,	Nízká	Střední	1	1	2	2	1	Zavedení malwaru
3	Cloudová infrastruktura	nedostatečné bezpečnostní povědomí uživatelů a ac	Střední	zneužití identity,	Nízká	Střední	2	1	2	4	2	Falešná identita
4	Cloudová infrastruktura	nevhodné nastavení přístupových oprávnění,	Střední	zneužití identity,	Nízká	Střední	2	1	2	4	2	Miskonfigurace přístupových práv
5	Cloudová infrastruktura	nedostatečné monitorování činnosti uživatelů a adn	Nízká	zneužití nebo neoprávněná modifikace údajů,	Nízká	Nízký	1	1	1	1	1	Auditní logy
6	Cloudová infrastruktura	nedostatečné stanovení bezpečnostních pravidel, ne	Nízká	pochybení ze strany zaměstnanců,	Střední	Nízký	1	2	1	2	1	Dokumentace
7	Osobní počítač	nedostatečná údržba informačního a komunikačníh	Střední	porušení bezpečnostní politiky, provedení neoprávněných činností, zneužití oprávnění ze strany uživatelů a administrátorů,	Nízká	Nízký	2	1	1	2	1	Zneužití osobních počítačů
8	Osobní počítač	zastaralost informačního a komunikačního systému,	Střední	poškození nebo selhání technického anebo programového vybavení,	Nízká	Nízký	2	1	1	2	1	Zastaralost počítačového vybavení
9	Osobní počítač	nevhodné nastavení přístupových oprávnění,	Střední	zneužití nebo neoprávněná modifikace údajů,	Nízká	Střední	2	1	2	4	2	Modifikace dat
10	Osobní počítač	nedostatečné bezpečnostní povědomí uživatelů a ac	Nízká	porušení bezpečnostní politiky, provedení neoprávněných činností, zneužití oprávnění ze strany uživatelů a administrátorů,	Nízká	Nízký	1	1	1	1	1	Nízké povědomí uživatelů o užití výpočetní techniky
11	Osobní počítač	nedostatečné monitorování činnosti uživatelů a adn	Nízká	škodlivý kód (například viry, spyware, trojské koně),	Střední	Střední	1	2	2	4	2	Zavedení malwaru
12	Osobní počítač	nedostatečné postupy při identifikování a odhalení	Nízká	užívání programového vybavení v rozporu s licenčními podmínkami,	Nízká	Nízký	1	1	1	1	1	Nelicencovaný software
13	Osobní počítač	neschopnost včasného odhalení pochybení ze stran	Střední	cílený kybernetický útok pomocí sociálního inženýrství, použití špionážních technik,	Nízká	Vysoký	2	1	3	6	2	Sociální inženýrství
14	Katalog družicových dat	nedostatečná ochrana aktiv,	Nízká	nedodržení smluvního závazku ze strany dodavatele,	Nízká	Vysoký	1	1	3	3	1	Selhání dodavatele
15	Mapový server	nedostatečná ochrana aktiv,	Nízká	nedodržení smluvního závazku ze strany dodavatele,	Nízká	Vysoký	1	1	3	3	1	Selhání dodavatele
16	Analytický výpočetní framework	nedostatečná údržba informačního a komunikačníh	Střední	škodlivý kód (například viry, spyware, trojské koně),	Nízká	Vysoký	2	1	3	6	2	Zavedení malwaru
17	Analytický výpočetní framework	nedostatečná údržba informačního a komunikačníh	Střední	poškození nebo selhání technického anebo programového vybavení,	Nízká	Vysoký	2	1	3	6	2	Selhární programového vybavení
18	Analytický výpočetní framework	neschopnost včasného odhalení pochybení ze stran	Nízká	zneužití vnitřních prostředků, sabotáž,	Nízká	Vysoký	1	1	3	3	1	Sabotáž zaměstnanců
19	Provozovatel cloudové infrastruktury	nedostatečná ochrana aktiv,	Nízká	dlouhodobé přerušení poskytování služeb elektronických komunikací, dodávky elektrické energie nebo jiných ležitých služeb,	Nízká	Vysoký	1	1	3	3	1	Přerušení poskytování klíčové služby
20	Provozovatel cloudové infrastruktury	nedostatečná ochrana aktiv,	Nízká	nedodržení smluvního závazku ze strany dodavatele,	Nízká	Vysoký	1	1	3	3	1	Přerušení poskytování klíčové služby

Risk Identification											
Risk ID	Date of Recording	Name of Risk Recorder	Risk Owner	Risk Title	Risk Description	Risk Category	Risk	Risk Cause	Likelihood (1 Very Low - 5 Very High)	Impact	Risk Lkelihood * Impact
R01-03	20-Mar-2024	XYZ	XYZ	Use Of Unlicensed Software (adobe)	Unlicensed software especially utility software may have source code vulnerability that can be exploited	Compromise of information	Unavailability or loss of information	No budget	Low	Minor	Low
R01-03	20-Mar-2024	XYZ	XYZ	Use Of Unlicensed Software (Microsoft)	Unlicensed software especially utility software may have source code vulnerability that can be exploited	Compromise of information	Unavailability or loss of information	No budget	Very low	Moderate	Low
R02-01	20-Mar-2024	XYZ	XYZ	Non-functioning website	The risk involves the potential for a website to become inaccessible or unresponsive as a result of deliberate attempts to overwhelm its servers with excessive traffic, impacting its functionality and availability to users.	Cyber attack risks	Denial-of-service attacks	Attack by hackers, bots	Low	Minor	Low
R02-02	20-Mar-2024	XYZ	XYZ	Ransomware	The risk entails the potential infiltration of ransomware into the organization's systems via deceptive phishing emails, posing a threat of data encryption and extortion.	Cyber attack risks	Introduction of ransomware through phishing	Careless employee	Moderate	Moderate	Medium
R02-04	20-Mar-2024	XYZ	XYZ	Unauthorized access	The risk involves the potential threat of unauthorized individuals gaining access to critical information systems, networks, and websites through malicious cyber attacks.	Cyber attack risks	Unauthorized access to information systems, networks, sites	Granting access rights to an unauthorised person	Very low	Moderate	Low
R02-05	20-Mar-2024	XYZ	XYZ	Intrusion from remote access points	The risk encompasses the potential threat of unauthorized entry into systems and networks via remote access points, increasing vulnerability to cyber attacks.	Cyber attack risks	Intrusion from remote access points	Unprotected access to the system	Very low	Moderate	Low
R02-06	20-Mar-2024	XYZ	XYZ	Malware	The risk encompasses the potential threat of malicious software infiltrating systems and networks, posing significant cybersecurity risks via employees activity	Cyber attack risks	Malware attacks	Insufficiently educated employees	Very low	Minor	Very Low
R02-08	20-Mar-2024	XYZ	XYZ	Systém rights	This risk entails unauthorized exploitation or manipulation of system privileges, potentially leading to data breaches or system compromise.	Cyber attack risks	Abuse or forging of information system rights	Employee attack	Very low	Moderate	Low
R02-09	20-Mar-2024	XYZ	XYZ	Illegal banking remittance	This risk involves unauthorized transactions or transfers of funds through internet banking channels due to cyber attacks, potentially leading to financial losses and regulatory violations	Cyber attack risks	Illegal remittance by internet banking	Employee or hacker attack	Very low	Moderate	Low

Hlava VI ZoKB

Přestupky

Naše znalosti pro Váš úspěch

Významná služba

- **poruší podmínku nebo zákaz** uložený Úřadem v opatření obecné povahy
- **nezjišťuje informace o dodavateli** bezpečnostně významné dodávky
- **neeviduje informace o dodavateli** bezpečnostně významné dodávky
- neohlásí Úřadu informace o dodavateli bezpečnostně významné dodávky nebo jejich změnu
- nezajišťuje dostupnost strategicky významné služby z území České republiky ve stanoveném čase a kvalitě
- **neprověřuje schopnost zajištění poskytování strategicky významné služby**

registrace jmen domén

- **nenahlásí Úřadu údaje** nebo jejich změnu
- neshromažďuje nebo neuchovává přesné a úplné údaje o registraci jmen **domén ve vyhrazené databázi**
- nezavede nebo nezveřejní **zásady a postupy zajišťující přesnost a úplnost informací** vedených v databázi, včetně postupů ověřování
- bez zbytečného odkladu po registraci jména domény neuveřejní její registrační údaje, které nejsou osobními údaji
- **neposkytne přístup ke konkrétním údajům o registraci jména domény**

Orgán nebo osoba

- **neposkytne součinnost** při zajišťování podkladů pro vydání protiopatření
- **nepředá data a informace**
- neposkytne informace na základě žádosti Úřadu podle neposkytne informace nebo jinou součinnost nezbytnou k posouzení naplnění kritérií regulované služby
- **neposkytnou součinnost při zvládání incidentu**
- neplní některou z povinností uloženou rozhodnutím o uložení nápravného opatření
- neposkytne vyžadované informace
- **nedodrží zákaz používání technických aktiv**
- neprovede opatření a neoznámí jeho výsledek Úřadu
- **neprovede sken zranitelností nebo penetrační test** (stav kybernetického nebezpečí)
- nezpřístupní neveřejnou komunikační síť v jeho správě
- neuveřejní informace o vyhlášení stavu kybernetického nebezpečí a o opatřeních
- neposkytne součinnost

Správce registru domény nejvyšší úrovně

- **neshromažďuje nebo neuchovává přesné a úplné údaje o registraci jmen domén** ve vyhrazené databázi
- nezavede nebo nezveřejní **zásady a postupy zajišťující přesnost a úplnost informací** vedených v databázi, včetně postupů ověřování
- bez zbytečného odkladu po registraci jména domény neuveřejní její registrační údaje, které nejsou osobními údaji
- **neposkytne přístup ke konkrétním údajům o registraci jména domény**

Fyzická osoba se dopustí přestupku tím, že poruší povinnost mlčenlivosti

Detaily analýzy rizik č. 9

Hledat | Nástroje vyhledávání | Smazat

ID	Aktivum	Maximální hodnota dostupnosti	Maximální hodnota důvěrnosti	Maximální hodnota integrity	Maximální hodnota zranitelnosti	Maximální hodnota hrozby	Maximální dopad dostupnost	Maximální dopad důvěrnost	Maximální dopad integrita	Počet druhů zranitelností	Počet druhů hrozeb	Počet navržených opatření	Akce
1	A1: Informatici	1	4	3	3	4	12	48	36	10	16	0	
2	A2: Outlook	N/A	N/A	N/A	3	4	-	-	-	10	16	0	
12	A12: Router 56	N/A	N/A	N/A	3	4	-	-	-	10	16	0	
13	A13: CRM	1	1	2	3	4	12	12	24	9	16	0	
14	A14: Notebook	N/A	N/A	N/A	3	4	-	-	-	9	16	0	
15	A15: Účetní program	N/A	N/A	N/A	3	4	-	-	-	9	16	0	
16	A16: Aktivum 1	N/A	N/A	N/A	3	4	-	-	-	9	16	0	
17	A17: Aktivum 2	N/A	N/A	N/A	3	4	-	-	-	9	16	0	
18	A18: Aktivum 3	N/A	N/A	N/A	3	4	-	-	-	9	16	0	
19	A19: Aktivum	N/A	N/A	N/A	3	4	-	-	-	9	16	0	
20	A20: Aktivum	N/A	N/A	N/A	3	4	-	-	-	6	16	0	
21	A21: Aktivum 6	N/A	N/A	N/A	3	4	-	-	-	8	16	0	
22	A22: Aktivum 7	N/A	N/A	N/A	3	4	-	-	-	6	16	0	
23	A23: Aktivum 8	N/A	N/A	N/A	3	4	-	-	-	6	16	0	

A18: Aktivum
Aktivum 3

Detaily analýzy rizik č. 9

Hledat | Nástroje vyhledávání | Smazat

ID	Aktivum	Maximální hodnota dostupnosti	Maximální hodnota důvěrnosti	Maximální hodnota integrity	Maximální hodnota zranitelnosti	Maximální hodnota hrozby	Maximální dopad dostupnost	Maximální dopad důvěrnost	Maximální dopad integrita	Počet druhů zranitelností	Počet druhů hrozeb	Počet navržených opatření	Akce
1	A1: Informatici	1	4	3	3	4	12	48	36	10	16	0	

ID	Aktivum	Hodnota dopadu dostupnost	Hodnota dopadu důvěrnost	Hodnota dopadu integrita	Zranitelnost	Hodnota zranitelnosti	Hrozba	Hodnota hrozby	Hodnota rizika dostupnost	Hodnota rizika důvěrnost	Hodnota rizika integrita	Způsob zvládání rizika	Vlastník rizika	Akce
2704	A1: Informatici	1	4	3	Z1: Nedostatečná údrž…	-	H1: Porušení …	3	N/A	N/A	N/A			
2705	A1: Informatici	1	N/A	3	Z1: Nedostatečná údrž…	-	H2: Poškoze…	-	N/A	N/A	N/A			
2706	A1: Informatici	1	4	3	Z1: Nedostatečná údrž…	-	H3: Zneužití i…	4	N/A	N/A	N/A			
2707	A1: Informatici	1	4	3	Z1: Nedostatečná údrž…	-	H5: Působení…	-	N/A	N/A	N/A			
2708	A1: Informatici	1	4	3	Z1: Nedostatečná údrž…	-	H6: Narušení …	-	N/A	N/A	N/A			
2709	A1: Informatici	1	N/A	3	Z1: Nedostatečná údrž…	-	H7: Přerušení…	-	N/A	N/A	N/A			
2710	A1: Informatici	1	4	3	Z1: Nedostatečná údrž…	-	H8: Zneužití …	-	N/A	N/A	N/A			
2711	A1: Informatici	1	4	N/A	Z1: Nedostatečná údrž…	-	H9: Ztráta, od…	-	N/A	N/A	N/A			
2712	A1: Informatici	1	4	3	Z1: Nedostatečná údrž…	-	H11: Pochyb…	-	N/A	N/A	N/A			
2713	A1: Informatici	1	N/A	N/A	Z1: Nedostatečná údrž…	-	H12: Zneužití…	-	N/A	N/A	N/A			
2714	A1: Informatici	1	N/A	N/A	Z1: Nedostatečná údrž…	-	H13: Dlouhod…	-	N/A	N/A	N/A			
2715	A1: Informatici	1	4	3	Z1: Nedostatečná údrž…	-	H15: Cílený k…	2	N/A	N/A	N/A			

Detaily analýzy rizik č. 9

Hledat | Nástroje vyhledávání | Smazat

ID	Aktivum	Maximální hodnota dostupnosti	Maximální hodnota důvěrnosti	Maximální hodnota integrity	Maximální hodnota zranitelnosti	Maximální hodnota hrozby	Maximální dopad dostupnost	Maximální dopad důvěrnost	Maximální dopad integrita	Počet druhů zranitelností	Počet druhů hrozeb	Počet navržených opatření	Akce
2707	A1: Informatici	1	4	3	Z1: Nedostatečná údrž…	-	H5: Působení…	-	N/A	N/A	N/A		
2708	A1: Informatici	1	4	3	Z1: Nedostatečná údrž…	-	H6: Narušení …	-	N/A	N/A	N/A		
2709	A1: Informatici	1	N/A	3	Z1: Nedostatečná údrž…	-	H7: Přerušení…	-	N/A	N/A	N/A		
2710	A1: Informatici	1	4	3	Z1: Nedostatečná údrž…	-	H8: Zneužití …	-	N/A	N/A	N/A		
2711	A1: Informatici	1	4	N/A	Z1: Nedostatečná údrž…	-	H9: Ztráta, od…	-	N/A	N/A	N/A		
2712	A1: Informatici	1	4	3	Z1: Nedostatečná údrž…	-	H11: Pochyb…	-	N/A	N/A	N/A		
2713	A1: Informatici	1	N/A	N/A	Z1: Nedostatečná údrž…	-	H12: Zneužití…	-	N/A	N/A	N/A		
2714	A1: Informatici	1	N/A	N/A	Z1: Nedostatečná údrž…	-	H13: Dlouhod…	-	N/A	N/A	N/A		
2715	A1: Informatici	1	4	3	Z1: Nedostatečná údrž…	-	H15: Cílený k…	2	N/A	N/A	N/A		

Opatření k riziku č.2704

Kamerové systémy
Pravidelné zálohování
Mříže
Firewally (Všechny typy)
Školení uživatelů

Hlava VI ZoKB

Přestupky - certifikace

Naše znalosti pro Váš úspěch

Držitel evropského certifikátu kybernetické bezpečnosti se dopustí přestupku tím, že neinformuje příslušné subjekty posuzování shody o veškerých později zjištěných zranitelnostech nebo nesrovnalostech

Vnitrostátní orgán certifikace kybernetické bezpečnosti – NÚKIB

NÚKIB bude dohlížet na dodržování pravidel zahrnutých v evropských systémech certifikace kybernetické bezpečnosti a tato pravidla vymáhat, napomáhat Českému institutu pro akreditaci při monitorování činnosti subjektů posouvání shody, v příslušných případech autorizovat nebo pověřovat subjekty posuzování shody k udělování certifikací a řešit stížnosti podané fyzickými nebo právnickými osobami v souvislosti s evropskými certifikáty kybernetické bezpečnosti.

Vnitrostátní subjekt akreditace – Český institut pro akreditaci (ČIA)

ČIA je akreditačním orgánem, který bude akreditovat subjekty posuzování shody. Na základě této akreditace budou subjekty posuzování shody oprávněny udělovat certifikace kybernetické bezpečnosti, vyjma případů s potřebnou autorizací. ČIA je pověřen k provádění akreditace ve smyslu nařízení Evropského parlamentu a Rady (ES) č. 765/2008 rozhodnutím Ministerstva průmyslu a obchodu ČR.

Agentura Evropské unie pro kybernetickou bezpečnost (ENISA)

ENISA vypracovává návrhy systémů certifikace pro konkrétní produkty, služby a procesy. Dále může zřizovat ad hoc pracovní skupiny pro zpracovávání návrhů certifikačních systémů. ENISA bude také provozovat internetovou stránku poskytující informace o evropských systémech certifikace kybernetické bezpečnosti, o evropských certifikátech kybernetické bezpečnosti a EU *prohlášeních o shodě*, včetně informací o zrušení a pozbytí platnosti těchto certifikátů a prohlášení.

Subjekty posuzování shody (CABs)

Subjekt, který uděluje certifikace v rámci daného certifikačního systému. CAB musí získat akreditaci udělovanou ČIA, případně také autorizaci udělovanou NÚKIB.

Evropská skupina pro certifikaci kybernetické bezpečnosti (ECCG)

ECCG se skládá ze zástupců vnitrostátních orgánů certifikace kybernetické bezpečnosti nebo jiných příslušných vnitrostátních orgánů. Hlavními úkoly skupiny je poskytovat poradenství a pomoc Komisi a ENISA při uplatňování evropského rámce pro certifikaci kybernetické bezpečnosti. ECCG může navrhovat nové systému EU certifikací či připomínkovat stávající návrhy certifikačních systémů.

Hlava VI ZoKB

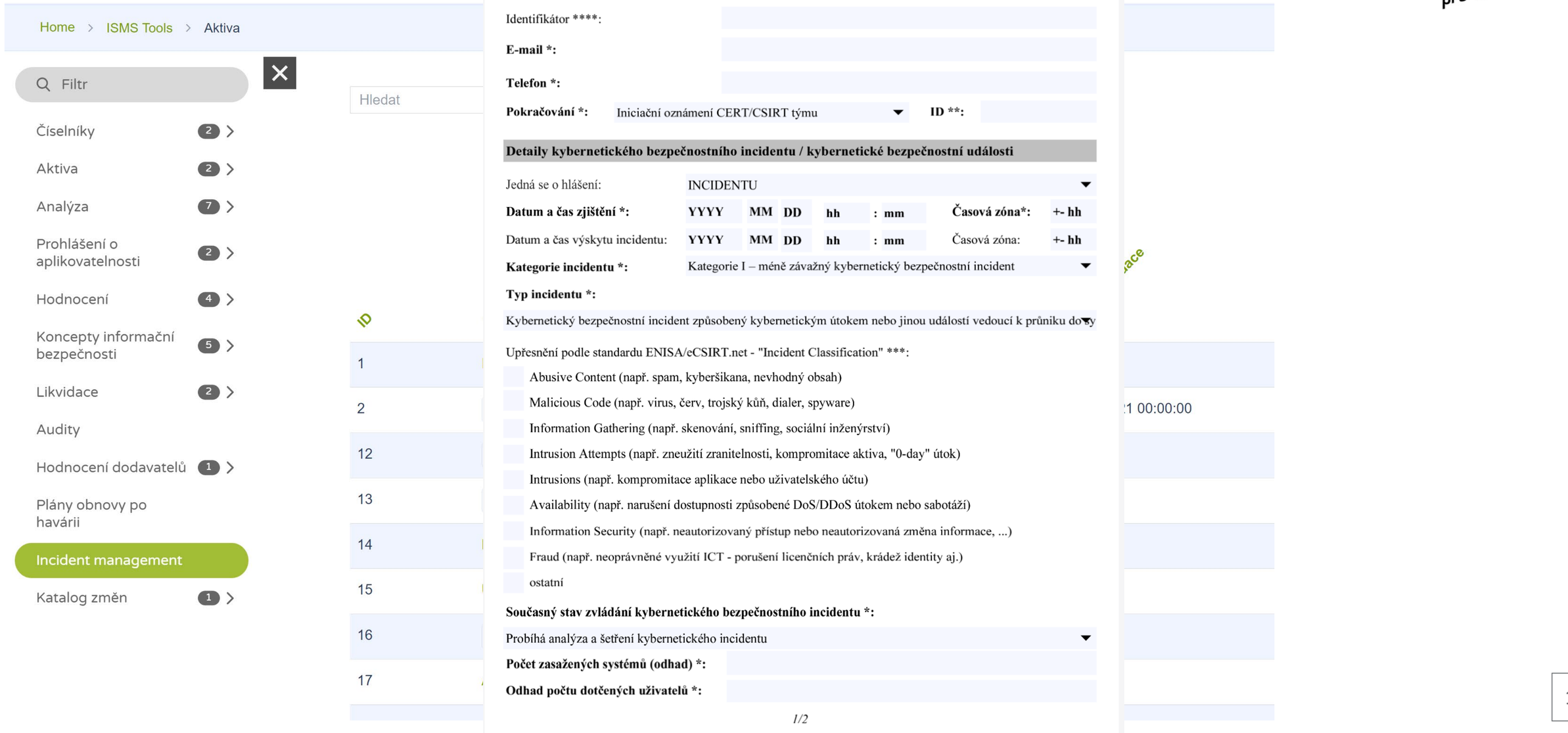
Přestupky

Entita vydávající Prohlášení o shodě

- **vydá EU prohlášení o shodě, ač pro jeho vydání nejsou splněny podmínky** stanovené aktem o kybernetické bezpečnosti,
- neuchovává dokumenty a informace podle čl. 53 odst. 3 aktu o kybernetické bezpečnosti,
- nepředloží vyhotovení EU prohlášení o shodě Úřadu a agentuře ENISA podle čl. 53 odst. 3 aktu o kybernetické bezpečnosti, nebo
- neposkytuje informace o kybernetické bezpečnosti v rozsahu a způsobem uvedeným v čl. 55 aktu o kybernetické bezpečnosti.

Právnická nebo podnikající fyzická osoba

- **zneužije známku nebo označení evropského systému certifikace** kybernetické bezpečnosti, evropský certifikát kybernetické bezpečnosti, EU prohlášení o shodě anebo jiný dokument podle aktu o kybernetické bezpečnosti,
- **padělá nebo pozmění evropský certifikát** kybernetické bezpečnosti, EU prohlášení o shodě anebo jiný dokument podle aktu o kybernetické bezpečnosti,
- provede činnost posouzení shody podle aktu o kybernetické bezpečnosti na úroveň záruky „vysoká“, přestože k tomu není oprávněna
- jako autorizovaný subjekt posuzování shody vydá evropský certifikát kybernetické bezpečnosti k produktu, procesu nebo službě, které nesplňují kritéria obsažená v přímo použitelném předpise Evropské unie přijatém na základě aktu o kybernetické bezpečnosti,
- **provede bez autorizace činnost posouzení shody**, vyhrazenou přímo použitelným předpisem Evropské unie přijatém na základě aktu o kybernetické bezpečnosti autorizovanému subjektu posuzování shody,
- **vystupuje jako akreditovaný subjekt posuzování shody bez akreditace** nebo mimo rozsah této akreditace
- jako subjekt posuzování shody nesplní Úřadem uloženou povinnost pozastavit platnost jím vydaného certifikátu nebo osvědčení


Home > ISMS Tools > Aktiva
Filtr
Hledat
Číselníky 2
Aktiva 2
Analýza 7
Prohlášení o aplikovatelnosti 2
Hodnocení 4
Koncepty informační bezpečnosti 5
Likvidace 2
Audity
Hodnocení dodavatelů 1
Plány obnovy po havárii
Incident management
Katalog změn 1
ID
1
2
12
13
14
15
16
17
Formulář hlášení kybernetického bezpečnostního incidentu
Míra ochrany informace *: Neomezeno (veřejné)
Kontaktní údaje
Orgán a osoba uvedená v § 3 písm. c) a e) zákona *:
Identifikátor ****:
E-mail *:
Telefon *:
Pokračování *: Iniciační oznámení CERT/CSIRT týmu
ID **:
Detaily kybernetického bezpečnostního incidentu / kybernetické bezpečnostní události
Jedná se o hlášení: INCIDENTU
Datum a čas zjištění *: YYYY MM DD hh : mm Časová zóna*: +- hh
Datum a čas výskytu incidentu: YYYY MM DD hh : mm Časová zóna: +- hh
Kategorie incidentu *: Kategorie I – méně závažný kybernetický bezpečnostní incident
Typ incidentu *:
Kybernetický bezpečnostní incident způsobený kybernetickým útokem nebo jinou událostí vedoucí k průniku do
Upřesnění podle standardu ENISA/eCSIRT.net - "Incident Classification" ***:
Abusive Content (např. spam, kyberšikana, nevhodný obsah)
Malicious Code (např. virus, červ, trojský kůň, dialer, spyware)
Information Gathering (např. skenování, sniffing, sociální inženýrství)
Intrusion Attempts (např. zneužití zranitelnosti, kompromitace aktiva, "0-day" útok)
Intrusions (např. kompromitace aplikace nebo uživatelského účtu)
Availability (např. narušení dostupnosti způsobené DoS/DDoS útokem nebo sabotáží)
Information Security (např. neautorizovaný přístup nebo neautorizovaná změna informace, ...)
Fraud (např. neoprávněné využití ICT - porušení licenčních práv, krádež identity aj.)
ostatní
Současný stav zvládání kybernetického bezpečnostního incidentu *:
Probíhá analýza a šetření kybernetického incidentu
Počet zasažených systémů (odhad) *:
Odhad počtu dotčených uživatelů *:
1/2
1 00:00:00

Hlava VI ZoKB

Pokuty a sankce

Za přestupek lze uložit pokutu do výše

- **250 000 000 Kč** nebo jedná-li se o podnik podle čl. 101 a 102 Smlouvy o fungování Evropské unie, až do výše **2 % čistého celosvětového ročního obratu** dosaženého podnikem za bezprostředně předcházející účetní období, podle toho, která z daných částek je vyšší, jde-li o přestupek podle odstavce 1 písm. a), d) až k) a m) až p), odstavce 3 písm. a), e) a f), odstavce 6 písm. b) nebo odstavce 8 písm. b) (registrace, aktiva, bezpečnostní opatření, incidenty, součinnost, neplní požadavky, požadavky na dodavatele, nápravná opatření, nezajistí dostupnost, poruší zákaz)
- **175 000 000 Kč** nebo jedná-li se o podnik podle čl. 101 a 102 Smlouvy o fungování Evropské unie, až do výše **1,4 % čistého celosvětového ročního obratu** dosaženého podnikem za bezprostředně předcházející účetní období, podle toho, která z daných částek je vyšší, jde-li o přestupek podle odstavce 2 písm. a), d) až k) a m) až p) nebo odstavce 8 písm. c), d) a g), (registrace, aktiva, bezpečnostní opatření, incidenty, součinnost, neplní požadavky, požadavky na dodavatele, nápravná opatření, zranitelnosti a penetrační testy)
- **100 000 000 Kč**, jde-li o přestupek podle odstavce 1 písm. b), odstavce 3 písm. b) a c) nebo odstavce 8 písm. a) a f), (registrace a údaje, info o dodavateli, neposkytne informace)
- **50 000 000 Kč**, jde-li o přestupek podle odstavce 1 písm. c) a l), odstavce 2 písm. b), odstavce 3 písm. d), odstavce 4 písm. a) až e), odstavce 5 písm. a) až d), odstavce 6 písm. a), c) a d), odstavce 7 písm. a) a b), odstavce 8 písm. e) nebo odstavce 13 písm. a) (zastupitelnost a neoznámení o provedení protiopatření)
- **35 000 000 Kč**, jde-li o přestupek podle odstavce 2 písm. c) a l), (zastupitelnost a neoznámení o provedení protiopatření)
- **20 000 000 Kč**, jde-li o přestupek podle odstavce 13 písm. b) až d) nebo odstavce 14 písm. a) až c) a e) až g), (prohlášení o shodě)
- **2 000 000 Kč**, jde-li o přestupek podle odstavců 10, 11 a 12 nebo odstavce 14 písm. d) (komunita nebo neinformování držitelem certifikátu o zranitelnostech)
- **50 000 Kč**, jde-li o přestupek podle odstavce 9. (mlčenlivost)

Úřad může v případě nesplnění povinnosti odstranit organizaci v režimu vyšších povinností, která je držitelem evropského certifikátu kybernetické bezpečnosti nebo jiného certifikátu nebo osvědčení souvisejícího se zajištěním kybernetické bezpečnosti regulované služby, **pozastavit platnost certifikátu**

Soud může na návrh Úřadu rozhodnout, že člen statutárního orgánu organizace, která v přímé souvislosti s plněním rozhodnutí Úřadu, kterým byla v režimu vyšších povinností uložena povinnost odstranit zjištěné nedostatky, opakovaně nebo závažně porušila své povinnosti při výkonu své řídící funkce, v důsledku čehož bylo zmařeno řádné splnění rozhodnutí Úřadu, **nesmí až do doby odstranění zjištěných nedostatků , nejméně však po dobu 6 měsíců tuto řídicí funkci vykonávat.**

Informaci o pozastavení platnosti certifikátu nebo osvědčení či pozastavení výkonu řídící funkce **Úřad zveřejní na svých internetových stránkách**.

Metodika hodnocení dodavatelů

Ukázka jednoho z typů hodnocení v nástroji ISMS Tools

Naše znalosti pro Váš úspěch

Průběh řízení a společná ustanovení

Zajištění účelu a průběhu řízení

- Úřad může uložit **pořádkovou pokutu až do výše 100 000 Kč. Pořádkovou pokutu lze uložit i opakovaně**. Celková výše opakovaně ukládaných pokut **nesmí přesáhnout**
- **10 000 000 Kč nebo 1 % z čistého obratu** dosaženého právnickou nebo podnikající fyzickou osobou za poslední ukončené účetní období podle toho, která z daných částek je vyšší.
- Úřad může za účelem **vymáhání splnění povinnosti** uložené rozhodnutím Úřadu ukládat **donucovací pokuty až do výše 10 000 000 Kč nebo 1 % z čistého obratu** dosaženého právnickou nebo podnikající fyzickou osobou za poslední ukončené účetní období podle toho, která z daných částek je vyšší.
- Za přestupek, kterého se poskytovatel regulované služby dopustí tím, že jako **kontrolovaná osoba nesplní některou z povinností podle kontrolního řádu**, lze uložit pokutu do **10 000 000 Kč.**

Součinnost

- **Orgány veřejné moci jsou povinny** bez zbytečného odkladu, a nestanoví-li jiný právní předpis jinak, i bez úplaty **poskytnout Úřadu podněty, informace a jiné formy součinnosti** potřebné k výkonu pravomocí a za účelem splnění povinností Úřadu, které jsou stanoveny tímto zákonem. Orgány veřejné moci a Úřad při výkonu pravomocí svěřených Úřadu tímto zákonem vzájemně spolupracují, jsou oprávněny vyžadovat stanoviska k připravovaným rozhodnutím vydávaným v mezích jejich působnosti a usilují při tom o dosažení shody těchto stanovisek. Orgány veřejné moci a Úřad dále v rozsahu, který je nezbytný pro plnění úkolů orgánů veřejné moci a Úřadu, **sdílí informace o hrozbách, zranitelnostech a incidentech a o opatřeních** přijatých v reakci na tyto hrozby, zranitelnosti a incidenty. Ustanovení § 48 odst. 2 a 3 tím nejsou dotčena. **Plnění těchto povinností mohou orgány činné v trestním řízení v nezbytně nutném rozsahu omezit** nebo na nezbytně nutnou dobu odložit, pokud by poskytnutím součinnosti došlo k ohrožení či zmaření účelu trestního řízení.
- **Orgány a osoby**, u kterých lze důvodně předpokládat, že **naplňují kritéria pro identifikaci nebo určení regulované služby, jsou povinny bez zbytečného odkladu**, a nestanoví-li jiný právní předpis jinak, **i bez úplaty poskytnout informace nezbytné k posouzení naplnění kritérií regulované služby a další nezbytnou součinnost**. Požadovaná součinnost nemusí být poskytnuta, brání-li v tom zákonná nebo státem uznaná povinnost mlčenlivosti.
- Ministerstva a ústřední orgány bez zbytečného odkladu informují Úřad o určení prvků kritické infrastruktury a o důvodech určení.
- **Úřad je oprávněn od Generálního finančního ředitelství požadovat poskytnutí informací získaných při správě daní**
- **Úřad a Úřad pro ochranu osobních údajů jsou vzájemně oprávněny požadovat informace a vyžadovat spolupráci**
- Ministerstvo spravedlnosti umožníÚřadu získat způsobem umožňujícím dálkový přístup z **evidence skutečných majitelů úplný výpis platných údajů**

FORUM

Naše znalosti
pro Váš úspěch

Buďte s námi v kontaktu

Děkuji za pozornost.

FORUM

Naše znalosti
pro Váš úspěch

Adresa

Kaprova 42/14
110 00 Praha 1

Kontakt

Email: info@acresia.com
Prodej: obchod@acresia.com
Podpora: support@acresia.com

Telefon

Tel: +420 321 123 123
GSM: +420 737 291 478
Skype: acresia

ACRESIA
CONSULTING