CENTRÁLNÍ REGISTR ZBRANÍ

PRAVIDLA BEZPEČNÉHO CHOVÁNÍ UŽIVATELE SYSTÉMU CRZ

(Bezpečnostní pravidla)

Verze: 19. 8. 2021

1. ÚČEL DOKUMENTU

Tímto dokumentem se stanoví základní pravidla bezpečného chování externího uživatele informačního systému centrální registr zbraní (dále jen „systém CRZ“). Externím uživatelem systému CRZ (dále jen „uživatelem“) je:

1. osoba pověřená držitelem zbrojní licence k přístupu do systému CRZ,
2. osoba pověřená držitelem obecné muniční licence k přístupu do systému CRZ,
3. zaměstnanec Českého úřadu pro zkoušení zbraní a střeliva (ČÚZZS) pověřený k přístupu do systému CRZ.

2. PŘÍSTUPOVÉ KONTO

Uživatel se do systému CRZ může přihlásit jen tehdy, má-li zřízeno přístupové konto.

Uživatel se při přihlašování do systému CRZ autentizuje prostřednictvím přístupu se zaručenou identitou s využitím občanského průkazu se strojově čitelnými údaji a s kontaktním elektronickým čipem nebo jiným prostředkem pro elektronickou identifikaci (například bankovní identitou).

Poznámka:

Během přechodného období (viz zákon č. 261/2021 Sb.), tj. ***do 24. 7. 2022*** *se uživatel může při přihlašování do systému CRZ autentizovat i osobním komerčním certifikátem.*

3. PRAVIDLA BEZPEČNÉHO CHOVÁNÍ

Za účelem minimalizace případného napadení počítače a mobilních zařízení, ze kterých uživatel přistupuje do systému CRZ, virem nebo jiným škodlivým softwarem a maximalizace ochrany údajů v systému CRZ, uživatel dodržuje následující pravidla bezpečného chování:

1. **Chraňte své přihlašovací údaje**

   Své přihlašovací údaje (elektronickou identitu) nikdy nikomu nesdělujte, ani je neposílejte e-mailem nebo prostřednictvím sociálních sítí. Při přihlašování dbejte na soukromí a kontrolujte, že další osoby nemohou zaregistrovat vaše přihlašovací údaje. Nenechávejte svůj počítač či mobilní zařízení bez dozoru. Nikdy nepřistupujte do systému CRZ na veřejnosti (např. v dopravních prostředcích nebo v dohledu bezpečnostních kamer).

2. **Hlídejte si, odkud přistupujete do systému CRZ**

   Nepřistupujte do systému CRZ z počítače, o kterém si nemůžete být jisti, že na něm nejsou nainstalovány škodlivé programy. Rozhodně se vyvarujte jakýmkoliv veřejným počítačům (např. v internetových kavárnách). Vždy si v adresním řádku zkontrolujte, zda do systému CRZ přistupujete zabezpečeným připojením.

   Stránka (název webu) musí začínat **https://crz.policie.cz/** (důležité je „s“ na konci), případně vás na to upozorní samotný prohlížeč zelenou barvou nebo symbolem zamčeného zámku před názvem webu.

3. **Dávejte pozor na neznámé odkazy**

   Vyvarujte se klikání na neznámé odkazy na internetu a v e-mailu, které by vás dovedly na stránky připomínající přihlašovací formulář do systému CRZ. Pokud se vám zdá přihlašovací stránka jakkoliv podezřelá, kontaktujte pracoviště HelpDESK CRZ. Vždy si zkontrolujte, zda jste na správné webové stránce (viz bod 2).

4. **Podezřelé e-maily neotvírejte a mažte**

   Policie ČR vám nikdy nepošle e-mail s žádostí o sdělení vašich osobních údajů nebo údajů se kterými se přihlašujete do CRZ (uživatelské jméno, heslo, údaje k ověření elektronické identity,…). Otevírejte pouze e-maily od známých a očekávatelných odesílatelů. Podezřelé e-maily nejlépe rovnou mažte. Pokud jste je již otevřeli, neotevírejte přílohy a neklikejte na odkazy v nich obsažené.

5. **Chraňte se proti spamu**

   Používejte e-mailovou ochranu proti spamu. Většina emailových klientů (např. outlook) ji nabízí.

6. **Používejte a aktualizujte antivirový program i firewall**

   Svůj počítač i mobilní zařízení pravidelně kontrolujte antivirovým programem. Antivirový program nikdy nevypínejte, pravidelně jej aktualizujte a používejte jeho nejnovější verzi. Starší verze antivirových programů nemusí být dost účinné proti novým hrozbám. Pokud máte podezření, že váš počítač nebo mobilní zařízení bylo napadeno škodlivým softwarem (virem), nepoužívejte jej pro přístup do systému CRZ a kontaktujte svého IT specialistu.

7. **Aktualizujte pravidelně svůj počítač i mobilní zařízení**

   Pravidelně aktualizujte své programy i operační systém. Věnujte zejména pozornost aktualizacím používaného internetového prohlížeče. Instalace aktualizací neodkládejte. Používejte nejnovější verze operačních systémů. Starší verze mohou být hrozbou pro bezpečné připojení do systému CRZ.

8. **Mějte přehled o svých aktivitách v systému CRZ**

   Vědět jaké změny v systému CRZ jste naposledy provedl je nejlepší nástroj pro včasné varování. Pokud zaznamenáte jakoukoliv změnu svých záznamů, kterou jste neprovedl, kontaktujte pracoviště HelpDESK CRZ.

9. Sledujte novinky o bezpečnosti na internetu

Pravidelně sledujte nejnovější zprávy z oblasti bezpečnosti na internetu a dodržujte všechna doporučená opatření.

10. Máte podezření? Kontaktujte HelpDESK systému CRZ

Jakmile zpozorujete cokoliv podezřelého v souvislosti s vaším přístupem do systému CRZ nebo s vašimi záznamy v systému CRZ, kontaktujte neprodleně pracoviště HelpDESK

- telefon 974 836 312,
- e-mail crz.verifikace@pcr.cz.

Policejní prezidium ČR
ředitelství služby pro zbraně a bezpečnostní materiál
oddělení centrálního registru zbraní