

## Check list pre subjekty kategórie I podľa vyhlášky 179/2020

**Autor:** Vládna jednotka CSIRT

**Vypracoval:** Vládna jednotka CSIRT,  
Ministerstvo investícií, regionálneho rozvoja a  
informatizácie Slovenskej republiky

**Vydané dňa:** 16.04.2024

**Verzia:** 2.0

TLP: White

## Check list pre subjekty kategórie I podľa vyhlášky 179/2020

Tento dokument Vám umožní zistiť základný stav bezpečnosti Vašich IT systémov. Pomocou check listu viete odhaliť nedostatky zabezpečenia IT systémov na základe čoho ich viete odstrániť. V prípade, že ste zaznamenali podozrivú aktivitu na Vašich zariadeniach alebo v informačnom systéme, obráťte sa na Vládnú jednotu CSIRT.

Číslo	Operačný systém	Splnené	Poznámka
OS1	Používajte podporovaný operačný systém na pracovných staniciach (Windows 10 verzia 22H2, alebo aktuálnu verziu Windows 11. Na serverovej časti minimálne Windows Server 2016 a novší	<input type="checkbox"/>	
OS2	Ak používate iný operačný systém ako Microsoft Windows, musí byť podporovaný výrobcom. Pravidelne kontrolujte dostupnosť aktualizácií a systém udržiavajte aktuálny	<input type="checkbox"/>	
OS3	Pravidelne kontrolujte dostupnosť bezpečnostných aktualizácií a systém udržiavajte vždy aktuálny	<input type="checkbox"/>	
OS4	Ak to systém umožňuje, je potrebné nastaviť automatické aktualizácie operačného systému	<input type="checkbox"/>	
OS5	Pravidelne kontrolujte dostupnosť aktualizácií a aktualizujte BIOS zariadení	<input type="checkbox"/>	
OS6	Každý používateľ počítača musí mať vytvorený vlastný používateľský účet	<input type="checkbox"/>	
OS7	Účet administrátora musí byť samostatný, nevyužíva sa na bežné činnosti (používa sa len v prípade potreby)	<input type="checkbox"/>	
OS8	Bežný používateľ musí mať obmedzené práva v operačnom systéme	<input type="checkbox"/>	
OS9	Odporúčame používať lokálne konto na prístup do počítača (online konto nesie riziká)	<input type="checkbox"/>	
OS10	Vaše používateľské konto musí mať nastavené automatické zamknutie pri nečinnosti (maximálne 5 minút)	<input type="checkbox"/>	
OS11	Šetrič obrazovky je potrebné nastaviť tak, aby pri jeho vypnutí bolo potrebné znovu zadať heslo	<input type="checkbox"/>	
OS12	Mali by ste mať vypnutú funkciu rýchleho spustenia systému Windows	<input type="checkbox"/>	
OS13	Máte zapnutú kontrolu používateľského konta na úroveň predvolené alebo vyššie	<input type="checkbox"/>	
OS14	Váš operačný systém musí mať zapnutú bránu firewall	<input type="checkbox"/>	
OS15	Nesmiete mať povolený vzdialený prístup k počítaču (RDP) ani inú iniciáciu spojenia zo siete	<input type="checkbox"/>	
OS16	Odporúčame pravidelne zisťovať dostupnosť a inštalovať ovládače a firmware periférnych zariadení	<input type="checkbox"/>	
OS17	Odporúčame pravidelne zisťovať dostupnosť a inštalovať aktualizácie ovládačov zariadenia	<input type="checkbox"/>	

TLP: White

OS18	Počítač musí byť zabezpečený antivírusovým softvérom (Windows Defender alebo antivírus tretích strán)	<input type="checkbox"/>	
OS19	Antivírusový softvér musí byť pravidelne aktualizovaný	<input type="checkbox"/>	
OS20	Antivírusový softvér musí byť pravidelne spúšťaný na úplnú kontrolu zariadenia pred hrozbami	<input type="checkbox"/>	
OS21	V antivírusovom systéme je potrebné povoliť rezidentnú ochranu.	<input type="checkbox"/>	
OS22	V operačnom systéme by malo byť zakázané automatické spúšťanie pripojiteľných USB zariadení a médií	<input type="checkbox"/>	
<b>Číslo</b>	<b>Tvorba a uchovávanie hesiel</b>	<b>Splnené</b>	<b>Poznámka</b>
PM1	Každé používateľské konto musí mať nastavené vlastné, unikátne heslo	<input type="checkbox"/>	
PM2	Heslo musí byť komplexné, odporúčame minimálnu dĺžku 16 znakov	<input type="checkbox"/>	
PM3	Heslo sa musí pravidelne meniť (odporúčame 1x za 90 dní)	<input type="checkbox"/>	
PM4	Pri zmene hesla by sa nemali opakovať slová/frázy ako tie, ktoré ste už v minulosti použili	<input type="checkbox"/>	
PM5	Heslá nesmú byť asociovateľné s používateľom, nesmú mať slovníkový význam a nesmú byť vytvorené miernou modifikáciou predchádzajúcich hesiel	<input type="checkbox"/>	
PM6	Heslá nesmú byť uchovávané v elektronickej alebo papierovej podobe v nechránenom priestore. Ideálne je uchovávať ich iba v pamäti používateľa alebo v na to určených softvérových úložiskách (správca hesiel)	<input type="checkbox"/>	
PM7	V prípade, že existuje podozrenie na odhalenie hesla, je nutné vykonať zmenu hesla okamžite	<input type="checkbox"/>	
PM8	Odporúčame využívanie viacfaktorovej autentifikácie (Windows Hello, token, certifikát, a iné)	<input type="checkbox"/>	
<b>Číslo</b>	<b>Bezpečnosť dát</b>	<b>Splnené</b>	<b>Poznámka</b>
BD1	Nesťahujte dáta z neznámych zdrojov	<input type="checkbox"/>	
BD2	Ak musíte stiahnuť neznámy súbor, pred jeho otvorením vykonajte kontrolu antivírusovým programom	<input type="checkbox"/>	
BD3	Všetky dôležité dáta je potrebné si pravidelne zálohovať mimo počítača v šifrovanej podobe. Odporúčaný interval zálohovania je jeden mesiac pri menej dôležitých dátach, týždeň pri dôležitých dátach a každý deň pri veľmi dôležitých a kritických dátach.	<input type="checkbox"/>	
BD4	Zálohované a šifrované dáta ukladajte na miesto s obmedzeným prístupom (trezor, uzamykateľná skrinka, a iné)	<input type="checkbox"/>	
BD5	Zálohované dáta je potrebné pravidelne kontrolovať, či záloha prebehla v poriadku. Odporúčaný interval kontroly záloh je jeden mesiac	<input type="checkbox"/>	
BD6	Odporúčame používať šifrovanie systémového disku a aj odkladacích diskov v počítači (BitLocker, VeraCrypt a iné)	<input type="checkbox"/>	
BD7	Všetky citlivé dáta v počítači je potrebné uchovávať iba v šifrovanej podobe.	<input type="checkbox"/>	

TLP: White

BD8	Pred spustením alebo skopírovaním súboru (súborov) z neznámeho média je potrebné tieto súbory skontrolovať antivírusovým softvérom	<input type="checkbox"/>	
<b>Číslo</b>	<b>Bezpečnosť aplikácií</b>	<b>Splnené</b>	<b>Poznámka</b>
AS1	V balíčku kancelárskych programov (MS Office a jeho alternatívy, PDF prehliadače) musíte mať zakázané spúšťanie makro funkcií	<input type="checkbox"/>	
AS2	Nesťahujte aplikácie z neznámych a nedôveryhodných zdrojov	<input type="checkbox"/>	
AS3	Nainštalované aplikácie je potrebné pravidelne aktualizovať. Ak to aplikácia umožňuje, je potrebné ju nastaviť na automatické inštalovanie aktualizácií, prípadne nastaviť zobrazovanie upozornení na nové aktualizácie.	<input type="checkbox"/>	
AS4	Pravidelne vykonávajte kontrolu počítača a neznáme, alebo nepoužívané aplikácie odstráňte zo zariadenia	<input type="checkbox"/>	
AS5	Každá aplikácia má nastavené vlastné unikátne heslo (ak takúto funkcionality podporuje)	<input type="checkbox"/>	
AS6	Pravidelne meňte heslá k aplikáciám	<input type="checkbox"/>	
AS7	V aplikáciách nesmiete používať funkciu automatického ukladania hesiel	<input type="checkbox"/>	
AS8	Nespúšťajte aplikácie z neznámych zdrojov	<input type="checkbox"/>	
AS9	Ak aplikácia podporuje viacfaktorovú autentifikáciu, je potrebné ju využívať	<input type="checkbox"/>	
AS10	Je potrebné inštalovať a používať iba legálne aplikácie, ktoré sú získané iba z dôveryhodného zdroja. V prípade, že na stránke výrobcu je aj kontrolný súčet, je odporúčané tento kontrolný súčet overiť	<input type="checkbox"/>	
AS11	Rozšírenia do internetového prehliadača je vhodné inštalovať iba z dôveryhodných zdrojov	<input type="checkbox"/>	
<b>Číslo</b>	<b>Bezpečnosť na internete</b>	<b>Splnené</b>	<b>Poznámka</b>
IS1	Svoje heslá a prihlasovacie údaje nikdy nikam neposielajte e-mailom, chatom ani iným spôsobom. Nezdierajte ich so svojimi kolegami. V prípade, že prišla požiadavka aj zo zdanlivo dôveryhodného zdroja, je potrebné túto požiadavku odmietnuť a nahlásiť ju zodpovedným osobám ako bezpečnostný incident. Platí to najmä pre dôležité účty ako sú Internet Banking, prihlasovacie heslo do e-mailového konta, heslo pre účet administrátora počítača, či iné spravované účty organizácie	<input type="checkbox"/>	
IS2	Vždy navštevujte webové stránky ktoré sú zabezpečené protokolom <i>HTTPS</i> . Ak webová stránka nebude takto zabezpečená, webový prehliadač Vás na to zvyčajne upozorní	<input type="checkbox"/>	
IS3	Pokiaľ Vás prehliadač upozorní, že stránka nie je bezpečná, nepokúšajte sa ju napriek tomu otvárať	<input type="checkbox"/>	
IS4	Pri odchode z internetovej stránky sa najskôr z nej odhláste	<input type="checkbox"/>	

IS5	Neverte internetovým stránkam, ktoré ohlasujú výhry. Je veľká pravdepodobnosť, že tu existuje snaha o podvod. Nikde nezadávejte svoje údaje ako sú prihlasovacie mená, heslá alebo svoje osobné údaje	<input type="checkbox"/>	
IS6	Dbajte na zvýšenú opatrnosť pri emailových správach ktoré Vás citovo vydierajú, vyvíjajú na Vás nátlak, sľubujú výhry, finančnú odmenu, alebo od Vás žiadajú zadanie citlivých údajov	<input type="checkbox"/>	
IS7	Nikde na Internete by sa nemalo zadávať číslo platobnej karty, ani ďalšie údaje o platobnej karte, okrem prípadov, keď ňou chce používateľ platiť cez legitímnu platobnú bránu. Aj v tomto prípade je ale potrebná opatrnosť a využívanie služieb iba dôveryhodných elektronických obchodov	<input type="checkbox"/>	
IS8	Nevyužívajte ukladanie prístupových údajov v prehliadači	<input type="checkbox"/>	
IS9	Pravidelne kontrolujte dostupnosť a inštalujte aktualizácie internetových prehliadačov a ich doplnkov	<input type="checkbox"/>	
IS10	Nepoužívajte nepodporované internetové prehliadače (Internet Explorer)	<input type="checkbox"/>	
IS11	Neotvárajte neoverené a neznáme odkazy v emailoch	<input type="checkbox"/>	
IS12	Nesťahujte a neotvárajte prílohy v podozrivých emailoch	<input type="checkbox"/>	
<b>Číslo</b>	<b>Sieťová bezpečnosť</b>	<b>Splnené</b>	<b>Poznámka</b>
NS1	Používajte dostatočné zabezpečenie pre Wi-Fi sieť (minimálne WPA2 PSK)	<input type="checkbox"/>	
NS2	Wi-Fi sieť je zabezpečená minimálne 16 znakovým komplexným heslom (zabezpečené šifrovaním AES)	<input type="checkbox"/>	
NS3	Pravidelne meňte heslo k Wi-Fi sieti (minimálne raz za 12 mesiacov)	<input type="checkbox"/>	
NS4	Pravidelne kontrolujte dostupnosť a inštalujte aktualizácie firmvéru routeru	<input type="checkbox"/>	
NS5	Nezverejňujte heslo na Wi-Fi, okrem Wi-Fi siete určenej výhradne pre hostí	<input type="checkbox"/>	
NS6	Pre návštevy by ste mali mať vytvorenú samostatnú a oddelenú Wi-Fi sieť	<input type="checkbox"/>	
NS7	Odporúčame pravidelne kontrolovať, či poznáte zariadenia pripojené na Vašu Wi-Fi sieť	<input type="checkbox"/>	
NS8	Nikdy sa nepripájajte k neznámym Wi-Fi sieťam	<input type="checkbox"/>	
NS9	Ak máte inak vytvorený vzdialený prístup k pracovisku, alebo k dátam (VPN/SFTP/a iné), tento prístup musí byť zabezpečený šifrovaním a musí využívať viacfaktorovú autentifikáciu (osobné certifikáty, časovo obmedzené bezpečnostné kódy, a iné)	<input type="checkbox"/>	
NS10	Rozdeľte sieť/sieť na segmenty – zóny, a izolujte ich pomocou sieťových prvkov (napr. VLANy, podsieť, fyzickým oddelením atď.)	<input type="checkbox"/>	

NS11	Na hraniciach jednotlivých sietí/podsietí implementujte bránu/brány firewall pre filtrovanie sieťového toku a blokovanie nežiaducich alebo potenciálne škodlivých pripojení	<input type="checkbox"/>	
<b>Číslo</b>	<b>Školenie zamestnancov</b>	<b>Splnené</b>	<b>Poznámka</b>
ŠZ1	Pravidelné školenie zamestnancov o bezpečnostných hrozbách, phishingu, používaní silných hesiel a správnej reakcii na incidenty	<input type="checkbox"/>	
ŠZ2	Pravidelné preškolenie zamestnancov na implementované novinky v infraštruktúre (softvér, aplikácie, hardvér)	<input type="checkbox"/>	

TLP: White