MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

CSIRT.SK

Checklist 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:	14.04.2020
Verzia:	1.1

TLP: White

Checklist pre subjekty kategórie I podľa vyhlášky 179/2020

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

Číslo	Operačný systém	Splnené	Poznámka
OS1	Používajte podporovaný operačný systém (Windows 8.1, alebo aktuálnu verziu Windows 10)	☐	
OS2	Ak používate iný operačný systém ako Microsoft Windows, musí byť podporovaný výrobcom. Pravidelne kontrolujte dostupnosť aktualizácií a systém udržujte aktuálny	☐	
OS3	Pravidelne kontrolujte dostupnosť bezpečnostných aktualizácií a systém udržujte vždy aktuálny	☐	
OS4	Ak to systém umožňuje, je potrebné nastaviť automatické aktualizácie operačného systému	☐	
OS5	Pravidelne kontrolujte dostupnosť a aktualizujte BIOS počítača	☐	
OS6	Každý používateľ počítača musí mať vytvorený vlastný používateľský účet	☐	
OS7	Účet administrátora musí byť samostatný, nevyužíva sa na bežné činnosti (používa sa len v prípade potreby)	☐	
OS8	Bežný používateľ musí mať obmedzené práva v operačnom systéme	☐	
OS9	Odporúčame používať lokálne konto na prístup do počítača (online konto nesie riziká)	☐	
OS10	Vaše používateľské konto musí mať nastavené automatické zamknutie pri nečinnosti (maximálne 5 minút)	☐	
OS11	Šetrič obrazovky je potrebné nastaviť tak, aby pri jeho vypnutí bolo potrebné heslo.	☐	
OS12	Mali by ste mať vypnutú funkciu rýchleho spustenia systému Windows 10	☐	
OS13	Máte zapnutú kontrolu používateľského konta na úroveň predvolené alebo vyššie	☐	
OS14	Váš operačný systém musí mať zapnutú bránu firewall	☐	
OS15	Nesmiete mať povolený vzdialený prístup k počítaču (RDP) ani inú iniciáciu spojenia zo siete	☐	

OS16	Odporúčame pravidelne zisťovať dostupnosť a inštalovať ovládače periférnych zariadení	☐	
OS17	Odporúčame pravidelne zisťovať dostupnosť a inštalovať aktualizácie ovládačov zariadenia	☐	
OS18	Počítač musí byť zabezpečený antivírusovým softvérom	☐	
OS19	Antivírusový softvér musí byť pravidelne aktualizovaný	☐	

OS20	Antivírusový softvér musí byť pravidelne spúšťaný na úplnú kontrolu zariadenia pred hrozbami	☐	
OS21	V antivírusovom systéme je potrebné povoliť rezidentnú ochranu.	☐	
OS22	Operačný systém musí byť pravidelne zálohovaný na externý ukladací priestor, ktorý je odpojený od siete a bezpečne uložený na miesto s obmedzeným fyzickým prístupom	☐	
OS23	V operačnom systéme máte zakázané automatické spúšťanie pripojiteľných USB zariadení	☐	
OS23	V základnom stave by mali byť všetky služby zakázané a povoľujú sa len potrebné a zabezpečené služby	☐	
Číslo	**Tvorba a uchovávanie hesiel**	**Splnené**	**Poznámka**
PM1	Každé používateľské konto musí mať nastavené vlastné, unikátne heslo	☐	
PM2	Heslo musí byť komplexné s minimálnou dĺžkou 16 znakov	☐	
PM3	Heslo sa musí pravidelne meniť (minimálne 1x za 90 dní)	☐	
PM4	Pri zmene hesla nesmiete používať podobné slová/frázy ako tie, ktoré ste už niekde použili	☐	
PM5	Heslá nesmú byť asociovateľné s používateľom, nesmú mať slovníkový význam a nesmú byť vytvorené miernou modifikáciou predchádzajúcich hesiel.	☐	
PM6	Heslá nesmú byť uchovávané v elektronickej alebo papierovej podobe v nechránenom priestore. Ideálne je vhodné ich uchovávať iba v pamäti používateľa alebo v na to určených softvérových úložiskách (správca hesiel)	☐	
PM7	V prípade, že existuje podozrenie na odhalenie hesla, je nutné vykonať zmenu hesla okamžite	☐	
PM8	Ak je možné spolu s heslom nastaviť viacfaktorovú autentifikáciu, je potrebné ju využiť	☐	
Číslo	**Bezpečnosť dát**	**Splnené**	**Poznámka**
BD1	Nemali by ste sťahovať dáta z neznámych zdrojov	☐	

BD2	Ak musíte stiahnuť neznámy súbor, vykonáte jeho kontrolu antivírusovým programom	☐	
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.	☐	
BD4	Zálohované a šifrované dáta ukladajte na miesto s obmedzeným prístupom (trezor, uzamykateľná skrinka,...)	☐	
BD5	Zálohované dáta je potrebné pravidelne kontrolovať, či záloha prebehla v poriadku. Odporúčaný interval kontroly záloh je jeden mesiac	☐	

BD6	Odporúčame používať šifrovanie systémového disku a aj odkladacích diskov v počítači. (TrueCrypt, BitLocker,...)	☐	
BD7	Všetky citlivé dáta v počítači je potrebné uchovávať iba v šifrovanej podobe.	☐	
BD8	Pred spustením alebo skopírovaním súboru (súborov) z neznámeho média je potrebné tieto súbory skontrolovať antivírusovým softvérom	☐	
Číslo	**Bezpečnosť aplikácií**	**Splnené**	**Poznámka**
AS1	V balíčku kancelárskych programov (MS Office a jeho alternatívy) musíte mať zakázané spúšťanie makro kódov	☐	
AS2	Nesťahujte aplikácie z neznámych zdrojov	☐	
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.	☐	
AS4	Pravidelne vykonávajte kontrolu počítača a mažte neznáme, alebo nepoužívané aplikácie	☐	
AS5	Každá aplikácia (ktorá heslo vyžaduje) má nastavené vlastné, unikátne heslo	☐	
AS6	Pravidelne meňte heslá k aplikáciám	☐	
AS7	Pravidelne zálohujte aplikácie s citlivým, potrebným obsahom	☐	
AS8	V aplikáciách nesmiete používať funkciu automatického ukladania hesiel. Na tento účel slúži na to určený softvér (správca hesiel)	☐	
AS9	Nespúšťajte aplikácie z neznámych zdrojov	☐	
AS10	Ak aplikácia podporuje viacfaktorovú autentifikáciu, je potrebné ju využívať	☐	

AS11	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	☐	
AS12	Rozšírenia do internetového prehliadača je vhodné inštalovať iba z dôveryhodných zdrojov	☐	
Číslo	**Bezpečnosť na internete**	**Splnené**	**Poznámka**
IS1	Svoje heslá a prihlasovacie údaje nikdy nikam neposielajte e-mailom, chatom ani iným spôsobom. Nezdieľajte 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 zvlášť pre dôležité účty ako sú Internet Banking, prihlasovacie heslo do emailového konta, heslo pre účet administrátora počítača, či iné spravované účty organizácie	☐	
IS2	Pri prístupe na zabezpečené stránky prostredníctvom protokolu https je potrebné vždy overiť certifikát.	☐	
	Certifikát je viditeľný po kliknutí na zámok naľavo od adresy internetovej stránky		
IS3	Pokiaľ Vás prehliadač upozorní, že stránka nie je bezpečná, nepokúšajte sa na ňu ďalej dostať	☐	
IS4	Pri odchode z internetovej stránky je vždy potrebné sa z nej odhlásiť	☐	
IS5	Neverte internetovým stránkam, ktoré ohlasujú výhry. Je veľká pravdepodobnosť, že tu existuje snaha o podvod. Nikde nezadávajte svoje údaje ako sú prihlasovacie mená, heslá alebo svoje osobné údaje.	☐	
IS6	Dbajte na zvýšenú opatrnosť pri emailových správach sľubujúcich výhry, finančnú odmenu, alebo ak od Vás žiadajú zadanie citlivých údajov.	☐	
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.	☐	
IS8	Nevyužívajte ukladanie prístupových údajov v prehliadači	☐	
IS9	Pravidelne kontrolujte dostupnosť a inštalujte aktualizácie internetových prehliadačov	☐	
IS10	Nepoužívajte nepodporované internetové prehliadače (Internet Explorer)	☐	
IS11	Neotvárajte neoverené a neznáme odkazy v emailoch	☐	
IS12	Nesťahujte a neotvárajte prílohy v podozrivých emailoch	☐	

Číslo	Sieťová bezpečnosť	Splnené	Poznámka
NS1	Používajte dostatočné zabezpečenie pre WIFI sieť (WPA2 PSK)	☐	
NS2	WIFI sieť je zabezpečená minimálne 16 znakovým komplexným heslom (zabezpečené šifrovaním AES)	☐	
NS3	Pravidelne meňte heslo k WIFI sieti (minimálne raz za 12 mesiacov)	☐	
NS4	Pravidelne kontrolujte dostupnosť a inštalujte aktualizácie firmvéru routeru	☐	
NS5	Nezverejňujte heslo na WIFI, okrem WIFI siete určenej výhradne pre hostí	☐	
NS6	Pre návštevy by ste mali mať vytvorenú samostatnú, oddelenú WIFI sieť	☐	
NS7	Odporúčame pravidelne kontrolovať, či poznáte zariadenia pripojené na vašu WIFI sieť	☐	
NS8	Nikdy sa nepripájajte k neznámym WIFI sieťam		
NS9	Ak máte inak vytvorený vzdialený prístup k pracovisku, alebo k dátam (VPN/SFTP/...), tento prístup musí byť zabezpečený šifrovaním a musí využívať viacfaktorovú autentifikáciu (osobné certifikáty, časovo obmedzené bezpečnostné kódy,...)	☐	