Národní pedagogický institut České republiky

Auditní zpráva k digitální infrastruktuře školy

Příklad zprávy

Financováno Evropskou unií NextGenerationEU

Národní plán obnovy

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

Více informací
o činnosti IT guru

Národní pedagogický institut České republiky

Auditní zpráva k digitální infrastruktuře školy

1. Obecné informace, webové stránky a e-maily

Dne 30. 1. 2023 byl pracovníkem Národního pedagogického institutu České republiky proveden audit digitální infrastruktury školy. Zodpovědnou osobou na straně organizace. Audit porovnává stav v organizaci se Standardem konektivity[1] a klade důraz na zabezpečení perimetru, koncových bodů i síťové infrastruktury.
Používanými informačními systémy jsou Škola online, VIS, spisová služba.

Zjištěná rizika

Vážná rizika	
B 1.1	Zajistěte realizaci funkčního DMARC záznamu k ochraně e-mailových služeb.
B 1.2	Zajistěte vytvoření krizového týmu a vytvoření postupů pro krizové situace jako napadení malwarem, napadení hackery, ztráty důležitých zařízení (zničení, ztráta, vyhoření...), ztráty dat (útokem, úmyslným či neúmyslným smazáním...).
B 1.3	Zajistěte realizaci funkčního DKIM záznamu k ochraně e-mailových služeb.
B 1.4	Zajistěte provoz e-mailových služeb organizace na ověřené a zabezpečené službě (M365, Google ...) včetně antispamové ochrany.
B 1.5	Zajistěte nasazení systému pro evidenci servisních požadavků ITIL.
B 1.6	Zajistěte pravidelná školení uživatelů v oblasti používání HW i SW prostředků organizace.
B 1.7	Zajistěte pravidelná školení uživatelů v oblasti počítačové bezpečnosti.
B 1.8	Zajistěte vytvoření bezpečnostní politiky a směrnic, které budou platné pro uživatele počítačových prostředků.
Mírná rizika a doporučení	
C 1.1	Škola nedisponuje počítačovou jazykovou učebnou.
C 1.2	Doporučujeme mít přístup k prostoru, kde jsou umístěné webové stránky.
C 1.3	Škola nedisponuje polytechnickou učebnou.
C 1.4	Škola nedisponuje počítačovou učebnou přírodních věd.

Z celkových 43 bodů bylo získáno 19 bodů, tedy 44 %. Stav organizace v oblasti Obecné informace, webové stránky a e-maily je vážný.

Legenda stavu:
Kritický: 0–20 %, nebo v případě výskytu alespoň jednoho kritického rizika
Vážný: 21–75 %
Uspokojivý: 76–85 %
Velmi dobrý: více než 85 %

Financováno Evropskou unií
NextGenerationEU
Národní plán obnovy
MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

Národní pedagogický institut České republiky | Senovážné nám. 872/25, 110 00 Praha 1
Tel.: +420 222 122 112 | e-mail: sekretariat@npi.cz | IČ: 45768455 | DIČ: CZ45768455
Bankovní spojení: KB 79530011/0100

[1] Standard konektivity, verze červenec 2022, stáhnout

2. Firewall a připojení k internetu

Organizace je k internetové síti připojena rádiovým spojem s frekvencí 60 GHz s rychlostí stahování 120 Mbps a nahrávání 120 Mbps. Šíře pásma internetového připojení na jedno zařízení je 1,82 Mbps.

Zabezpečení perimetru sítě je zajištěno firewallem TP-LINK AX50.

Zjištěná rizika

Kritická rizika	
A 2.1	Nasaďte firewall s funkcí IPS nebo ji zapněte pro veškerou komunikaci přes firewall procházející.
Vážná rizika	
B 2.1	Nasaďte firewall s funkcí kontroly přístupu na webové stránky přes protokol TLS nebo ji zapněte pro veškerou komunikaci přes firewall procházející.
B 2.2	Nasaďte firewall s funkcí logování veškeré komunikace do internetu včetně identifikace uživatele nebo ji zapněte. Retence záznamů by měla být alespoň 3 měsíce.
B 2.3	Zajistěte vytvoření samostatné DMZ zóny pro veškerý přístup k veřejným službám v síti z internetu.
B 2.4	Nasaďte firewall s funkcí ATP nebo ji zapněte pro veškerou komunikaci přes firewall procházející.
B 2.5	Nasaďte firewall s funkcí kontroly přístupu aplikací na internet nebo ji zapněte pro veškerou komunikaci přes firewall procházející.
B 2.6	Nasaďte firewall s funkcí klientské VPN pro zabezpečený přístup uživatelů k prostředkům organizace nebo ji nastavte.
B 2.7	Nasaďte firewall s funkcí site-to-site VPN pro zabezpečený přístup mezi pobočkami či partnery nebo ji nastavte.
Mírná rizika a doporučení	
C 2.1	Zajistěte přístup k internetu protokolem IPv6.
C 2.2	Nasaďte firewall s funkcí nastavení pravidel včetně přístupu k internetu pro různé skupiny uživatelů samostatně nebo ji zapněte.
C 2.3	Nasaďte firewall s funkcí IDS nebo ji zapněte pro veškerou komunikaci přes firewall procházející.

Z celkových 41 bodů bylo získáno 16 bodů, tedy 39 %. Stav organizace v oblasti firewall a připojení k internetu je kritický.

Legenda stavu:
Kritický: 0–20 %, nebo v případě výskytu alespoň jednoho kritického rizika
Vážný: 21–75 %
Uspokojivý: 76–85 %
Velmi dobrý: více než 85 %

Financováno Evropskou unií
NextGenerationEU
Národní plán obnovy
MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

Národní pedagogický institut České republiky | Senovážné nám. 872/25, 110 00 Praha 1
Tel.: +420 222 122 112 | e-mail: sekretariat@npi.cz | IČ: 45768455 | DIČ: CZ45768455
Bankovní spojení: KB 79530011/0100

[1]Standard konektivity, verze červenec 2022, stáhnout

3. Síťová infrastruktura

Síťová infrastruktura je tvořena strukturovanou kabeláží s hvězdicovou topologií. Páteřní spoje jsou provedeny optickým vláknem nebo DAC kabelem. Kabelové rozvody propojuje 6 síťových přepínačů. Aktivní prvky kabelové sítě jsou centrálně spravovány. Síť sestává z jediného segmentu.

V organizaci je možné připojit se na bezdrátovou síť Wi-Fi. Prostory pokrývá 8 přístupových bodů. Bezdrátová infrastruktura je centrálně spravována.

Zjištěná rizika

Kritická rizika	
A 3.1	Zajistěte rozdělení síťového prostředí na bezpečnostní segmenty například využitím technologie 802.3Q VLAN. Rozdělení je potřeba minimálně pro infrastrukturu, koncové body připojené kabelovým spojením, Wi-Fi pro zařízení organizace, Wi-Fi pro BYOD zařízení, DMZ. Další v případě individuální potřeby.
A 3.2	Zajistěte kontrolu komunikace mezi bezpečnostními segmenty firewallem a omezte komunikaci pouze na potřebné služby.
A 3.3	Zajistěte systém auditování provozních a bezpečnostních záznamů v rozsahu IP adresa – čas – počítačový systém.
Vážná rizika	
B 3.1	Zajistěte oddělené Wi-Fi sítě pro zaměstnance školy, žáky a hosty.
B 3.2	Zajistěte přístup k Wi-Fi síti uživatelům organizace s využitím AES šifrování a protokolem 802.1X.
B 3.3	Zajistěte proměření realizované Wi-Fi sítě, případně před realizací zajistěte simulaci pokrytí na základě plánů budov organizace.
B 3.4	Zajistěte nasazení protokolu 802.1X pro přístup k síťovým prostředkům organizace.
B 3.5	Pořiďte ochranu proti výpadkům elektrické energie, podpětí a přepětí (UPS) pro aktivní síťové prvky.
B 3.6	Zajistěte nasazení technologie EDR/XDR pro vyhodnocování rozšířených hrozeb s využitím centrálního auditování provozních a bezpečnostních záznamů.
B 3.7	Nasaďte v organizaci DNSSEC validující resolver.
Mírná rizika a doporučení	
C 3.1	Doporučujeme nasadit protokol IPv6 v organizaci.
C 3.2	Doporučujeme nasadit NETFLOW sondu alespoň na internetové rozhraní.

Z celkových 68 bodů bylo získáno 33 bodů, tedy 49 %. Stav organizace v oblasti Síťová infrastruktura je kritický.

Legenda stavu:
Kritický: 0–20 %, nebo v případě výskytu alespoň jednoho kritického rizika
Vážný: 21–75 %
Uspokojivý: 76–85 %
Velmi dobrý: více než 85 %

Financováno Evropskou unií
NextGenerationEU
Národní plán obnovy
MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

Národní pedagogický institut České republiky | Senovážné nám. 872/25, 110 00 Praha 1
Tel.: +420 222 122 112 | e-mail: sekretariat@npi.cz | IČ: 45768455 | DIČ: CZ45768455
Bankovní spojení: KB 79530011/0100

[1]Standard konektivity, verze červenec 2022, stáhnout

4. Servery, síťová úložiště a data

V prostředí se nachází 1 fyzický server.

Zjištěná rizika

Kritická rizika	
A 4.1	Zajistěte každodenní automatické zálohování serverové infrastruktury.
A 4.2	Zajistěte systém zálohování principem 3-2-1. Tedy tři zálohy, dva různé typy úložišť, alespoň jedna záloha mimo organizaci (cloud).
A 4.3	Zajistěte každodenní automatické zálohování uživatelských dat.
A 4.4	Zajistěte ochranu serverů a síťových úložišť zárukou. Zvažte také rozšířený typ záruky pro servery a síťová úložiště například formou servisního zásahu druhý pracovní den.
A 4.5	Zajistěte provoz serverů ve virtualizovaném prostředí.
A 4.6	Zajistěte ochranu serverů a síťových úložišť proti přehřátí.
Vážná rizika	
B 4.1	Zajistěte rozdělení serverových rolí na jednotlivé virtuální servery, např. LDAP server, souborový server, databázový server, webový server atp.
B 4.2	Zajistěte centrální ukládání dat uživatelů na servery, síťová úložiště nebo cloudové služby.
B 4.3	Zajistěte pravidelné pokusné obnovy dat minimálně jednou za měsíc.
B 4.4	Zajistěte vysokou dostupnost důležitých serverů nebo zajistěte systém jejich plné obnovy.
B 4.5	Zajistěte ochranu serverů a síťových úložišť proti zaplavení.
B 4.6	Zajistěte ochranu serverů a síťových úložišť proti požáru.
Mírná rizika a doporučení	
C 4.1	Doporučujeme nasadit systém šifrování pro servery a síťová úložiště.

Z celkových 63 bodů bylo získáno 22 bodů, tedy 35 %. Stav organizace v oblasti Servery, síťová úložiště a data je kritický.

Legenda stavu:
Kritický: 0–20 %, nebo v případě výskytu alespoň jednoho kritického rizika
Vážný: 21–75 %
Uspokojivý: 76–85 %
Velmi dobrý: více než 85 %

Financováno Evropskou unií
NextGenerationEU
Národní plán obnovy
MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

Národní pedagogický institut České republiky | Senovážné nám. 872/25, 110 00 Praha 1
Tel.: +420 222 122 112 | e-mail: sekretariat@npi.cz | IČ: 45768455 | DIČ: CZ45768455
Bankovní spojení: KB 79530011/0100

[1]Standard konektivity, verze červenec 2022, stáhnout

5. Uživatelské účty a koncová zařízení

Organizace má 200 uživatelů. Jeden správce se stará o chod IT techniky.

V organizaci je využíváno 46 pevných počítačů, 17 notebooků, 20 tabletů, 12 interaktivních tabulí, 2 interaktivní displeje, 1 tiskárna formátu A3, 7 tiskáren formátu A4.

Zjištěná rizika

Kritická rizika	
A 5.1	Zajistěte centrální správu uživatelských účtů a jejich využívání na všech koncových zařízeních organizace.
A 5.2	Zajistěte každému zaměstnanci vlastní uživatelský účet.
A 5.3	Zajistěte každému studentovi vlastní uživatelský účet.
A 5.4	Zajistěte vícefaktorovou autentizaci pro uživatelské účty administrátorů.
A 5.5	Zajistěte zablokování lokálních administrátorských účtů nebo automatickou změnu hesel a jejich unikátnost mezi koncovými zařízeními.
A 5.6	Zajistěte vynucení složitosti hesel u všech uživatelských účtů.
A 5.7	Zajistěte centrální správu koncových zařízení.
Vážná rizika	
B 5.1	Zajistěte vícefaktorovou autentizaci pro uživatelské účty zaměstnanců.
B 5.2	Zajistěte nasazení systému šifrování pro koncová zařízení.
Mírná rizika a doporučení	
C 5.1	Doporučujeme zajistit možnost používat BYOD zařízení pro studenty školy. Jejich používání vyžaduje nastavení infrastruktury a bezpečnosti.

Z celkových 39 bodů bylo získáno 5 bodů, tedy 13 %. Stav organizace v oblasti Uživatelské účty a koncová zařízení je kritický.

Legenda stavu:
Kritický: 0–20 %, nebo v případě výskytu alespoň jednoho kritického rizika
Vážný: 21–75 %
Uspokojivý: 76–85 %
Velmi dobrý: více než 85 %

V kompletním skóre organizace z celkových 254 bodů získala 95 bodů, tedy 37 %. Celkový stav organizace je kritický.

Legenda celkového stavu:
Kritický: 0–20 %, nebo v případě výskytu alespoň jednoho kritického rizika
Vážný: 21–75 %
Uspokojivý: 76–85 %
Velmi dobrý: více než 85 %

Dne 15. 3. 2023
Audit provedl a vyhodnotil Tomáš Bazalík
Národní pedagogický institut České republiky

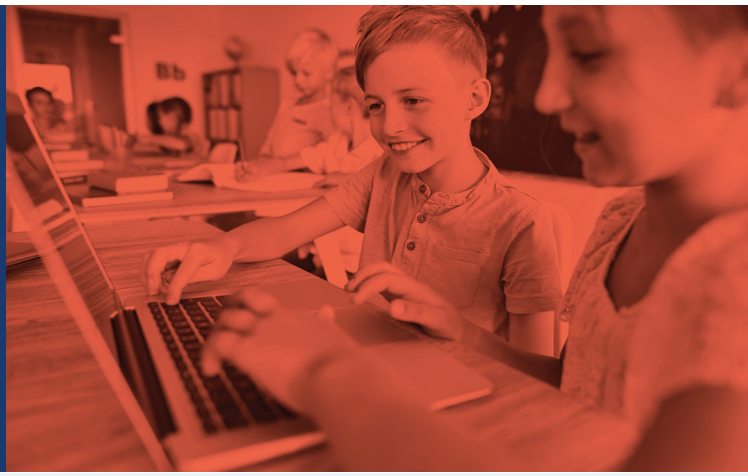
Financováno Evropskou unií
NextGenerationEU
Národní plán obnovy
MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

Národní pedagogický institut České republiky | Senovážné nám. 872/25, 110 00 Praha 1
Tel.: +420 222 122 112 | e-mail: sekretariat@npi.cz | IČ: 45768455 | DIČ: CZ45768455
Bankovní spojení: KB 79530011/0100

[1]Standard konektivity, verze červenec 2022, stáhnout

Národní pedagogický institut České republiky

Pomáháme školám při zavádění nové informatiky do výuky a rozvíjení digitálních kompetencí ve všech předmětech



V rámci projektu Národní plán obnovy 3.1 DIGI nabízíme zdarma různé formy podpory:

Vzdělávací kurzy a webináře

Přihlaste se do rozvíjejících vzdělávacích kurzů ze všech čtyř oblastí nové informatiky (kombinace prezenčního/online vzdělávání a e-learningu) a oborových kurzů k rozvoji digitálních kompetencí.

Individuální konzultace na míru

Konzultant vám poradí a navrhne možná řešení konkrétních problémů v souvislosti s úpravami ŠVP a zaváděním nové výuky. Konzultace lze čerpat opakovaně.

Workshopy pro celé sborovny

Specializovaní odborníci seznámí celý pedagogický sbor s revidovaným RVP ZV či G v nové informatice a digitálních kompetencích přímo u vás ve škole.

Sdílení dobré praxe (DIGI plovárny)

V bezpečném online prostředí získáte zkušenost od kolegů z jiných škol nebo můžete sdílet vlastní zkušenosti.

Konzultace od IT guru

Tým odborných nezávislých IT konzultantů vám doporučí vhodná řešení pro správu ICT vybavení školy, nastavení digitální infrastruktury sítě/konektivity, pomůže s nákupem digitálních technologií do výuky i se zabezpečením vnitřní sítě školy.

Konference

Na podzim pro vás připravujeme konference DigiSeč, Educa Liberec a také se podílíme na přípravě konference Škola jako místo setkávání, konkrétně garantujeme sekci Digitalizace vzdělávání.

DIGI roadshow

Několikrát do roka probíhají prezenční diskuzní setkání učitelů a ředitelů škol na krajských pracovištích NPI ČR.

Dále pro vás připravujeme kulaté stoly, podcasty KYBcast a DIGI IN nebo DigiPořad.

ZMĚNA JE ŽIVOT.
NEJSTE V TOM SAMI

Konkrétní informace najdete na webu revize.edu.cz

Financováno Evropskou unií NextGenerationEU
Národní plán obnovy
MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY