

Ukončení podpory Microsoft Windows 10: hrozby, udržitelnost a možná řešení

Lukáš Kozák



Univerzita Tomáše Bati ve Zlíně

Fakulta logistiky a krizového řízení

Ústav ochrany obyvatelstva

Akademický rok: 2024/2025

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	Lukáš Kozák
Osobní číslo:	L22233
Studijní program:	B1032A020002 Ochrana obyvatelstva
Forma studia:	Kombinovaná
Téma práce:	Ukončení podpory Microsoft Windows 10: hrozby, udržitelnost a možná řešení

Zásady pro vypracování

1. Zhodnotte vývoj a rozšíření operačních systémů společnosti Microsoft.
2. Popište bezpečnostní rizika spojená s používáním neaktualizovaných operačních systémů.
3. Blíže analyzujte podobné historické situace související s ukončením podpory operačních systémů.
4. Navrhněte vhodná opatření s ohledem na bezpečnost, udržitelnost a nákladovost.

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam doporučené literatury:

1. KOLOUCH, Jan. *Cybersecurtij*. Edice CZ.NIC, 2019. ISBN 978-80-88168-31-7.
2. KLATOVSKÝ, Karel. *Windows 11: Průvodce uživatele*, Grada, 2022. ISBN 978-80-271-3617-9
3. SEDLÁK, Petr a KONEČNÝ, Martin. *Kybernetická (ne)bezpečnost: problematika bezpečnosti v kyberprostru*. Vydání: první. Brno: CERM, akademické nakladatelství Aleš Čeněk, 2018. 978-80-7380-737-5.
4. ŠULC, Vladimír. *Kybernetická bezpečnost*. Plzeň: Bydavatelství a nakladatelství Aleš Čeněk, 2018. 978-80-7380-737-5.
5. YOSIFOVICH, Pavel; IONESCU, Alex ; RUSSINOVICH, Mark E. a SOLOMON, David A. *Windows Internals. Part 1, System architecture, processes, threads, memory managment, and more*. Seven edition. Redmond, Washington: Microsoft Press, 2017. ISBN 978-0735684188.

Další odborná literatura dle doporučení vedoucího bakalářské práce.

Vedoucí bakalářské práce: **Ing. Pavel Tomášek, Ph.D.**
Ústav ochrany obyvatelstva

Datum zadání bakalářské práce: **2. prosince 2024**

Termín odevzdání bakalářské práce: **2. května 2025**

L.S.

prof. Ing. Zuzana Tučková, Ph.D.
děkanka

prof. Ing. Dušan Vičar, CSc.
ředitel ústavu

V Uherském Hradišti dne 2. prosince 2024

PROHLÁŠENÍ AUTORA BAKALÁŘSKÉ PRÁCE

Beru na vědomí, že

- odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb., v platném znění bez ohledu na výsledek obhajoby;
- bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému a bude dostupná k nahlédnutí;
- jedno vyhotovení bakalářské práce v listinné podobě bude ponecháno Univerzitě Tomáše Bati ve Zlíně k uložení;
- na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- podle § 60 odst. 1 autorského zákona má Univerzita Tomáše Bati ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- podle § 60 odst. 2 a 3 mohu užít své dílo – bakalářskou práci – nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá; neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji, že

- jsem na bakalářské práci pracoval(a) samostatně a použitou literaturu jsem řádně citoval(a); v případě publikace výsledků budu uveden(a) jako spoluautor;
- odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou obsahově totožné.

V Uherském Hradišti, dne 2.5.2025.....
podpis autora

ABSTRAKT

Tato bakalářské práce je zaměřena na vyhodnocení bezpečnostních hrozeb v souvislosti s ukončením podpory systému Windows 10 v kontextu studovaného oboru Ochrany Obyvatelstva. Práce je uchopena jako historický náhled do vývoje daného softwaru operačního systému Windows, kdy dále v teoretické části jsou popsána bezpečnostní hrozby související s udržováním neaktualizovaného operačního systému v souvislosti s kyberbezpečností. V praktické části jsou dále analyzovány podrobné historické paralely týkající se ukončení podpory operačního systému Windows a dále je zde nabídnut souhrn technických možností, jež může pomoci nalézt řešení dané problematiky.

Klíčová slova: kyberbezpečnost, Ochrana obyvatelstva, ukončení podpory, Windows 10

ABSTRACT

This bachelor thesis focuses on the evaluation of security risks related to the discontinuation of Windows 10 support in the context of the studied field of Public Protection. The thesis is grasped as a historical insight into the development of the Windows operating system software in question, where further in the theoretical part the security risks associated with maintaining an un-updated operating system are described in the context of cyber security. The practical part further analyses detailed historical parallels related to the discontinuation of support for the Windows operating system and offers a summary of technical options that may help to find solutions to the issue.

Keywords: Protection of population , cyber security , end of support, Windows 10

V této bakalářské práci bych chtěl poděkovat za cenné rady a trpělivost svému vedoucímu práce panu doktorovi Ing. Ph.D. Pavlu Tomáškoví a dále velký dík patří samozřejmě i mé rodině, jež mě umožnila se soustředit na dané studium a všemožně mě podporovala a v neposlední řadě i svým kolegům a přátelům za rady, poznatky a podporu.

Dále děkuji všem ostatním, jež mi během studia či při psaní bakalářské práce poskytli podporu a zpětnou vazbu.

OBSAH

ÚVOD.....	11
I TEORETICKÁ ČÁST	12
1 VÝVOJ OPERAČNÍHO SYSTÉMU WINDOWS.....	13
1.1 SPOLEČNOST MICROSOFT	13
1.2 POČÁTKY SPOLEČNOSTI MICROSOFT	14
1.3 WINDOWS A JEHO JEDNOTLIVÉ VERZE	15
1.4 MINIMÁLNÍ SYSTÉMOVÉ NÁROKY WINDOWS 11	17
1.4.1 TPM 2.0.....	18
1.4.2 Podporované architektury procesorů.....	19
1.5 WINDOWS UPDATE	20
1.6 ROZŠÍŘENOST OS MS WINDOWS	21
2 ASPEKTY KYBERBEZPEČNOSTI	23
2.1 PRAVIDLA KYBERBEZPEČNOSTI	23
2.2 PROBLEMATIKA UDRŽENÍ SOFTWARE V AKTUÁLNÍ VERZI	24
2.3 DRUHY KYBERNETICKÝCH HROZEB.....	24
2.3.1 Malware.....	25
2.3.2 Ransomware	25
2.3.3 Phishing.....	26
2.3.4 Worm útok	26
2.3.5 Rootkit.....	26
3 PLATNÁ LEGISLATIVA V ČR, EU, SVĚTĚ	28
3.1 LEGISLATIVA V ČESKÉ REPUBLICCE	28
3.2 LEGISLATIVA V EVROPSKÉ UNII.....	28
3.3 LEGISLATIVA VE SVĚTĚ	29
3.4 NIS 2 APLIKOVÁNÍ SMĚRNICE V ČESKÉM PRÁVU	29
II PRAKTICKÁ ČÁST.....	31
4 HROZBY A HISTORICKÉ PARALELI	32
4.1 PŘÍADOVÁ STUDIE WANNACRY	32
4.2 PŘÍADOVÁ STUDIA NOTPETYA	35
4.3 VYHODNOCENÍ STUDIÍ.....	36
5 ANALÝZA SOUČASNÉHO STAVU A MOŽNOST ŘEŠENÍ	38
5.1 MOŽNOSTI ŘEŠENÍ SITUACE S UKONČENÍM PODPORY WINDOWS 10	38
5.1.1 Migrace na novější verzi operačního systému Windows 11	38
5.1.2 Využití programu ESU.....	39
5.1.3 Využití alternativního operačního systému.....	40
5.1.4 Cloudové řešení Azure	41

5.1.5	Virtualizace systému Windows 10.....	42
5.1.6	Off-line režim Windows.....	42
5.1.7	Instalace MS Windows 11 na nepodporované systémy	42
5.1.8	Setrvání na současné verzi Windows 10 i po ukončení podpory bez aktualizací.....	43
5.2	STRUKTUROVANÝ ROZHOVOR – ANTIVIROVÉ SPOLEČNOSTI	43
5.3	STRUKTUROVANÝ ROZHOVOR – SUBJEKTY KRITICKÉ INFRASTRUKTURY	45
6	MODELOVÁ SITUACE – KALKULACE.....	47
6.1	KALKULACE PŘI ŘEŠENÍ MIGRACE NA WINDOWS 11	47
6.2	KALKULACE PŘI ŘEŠENÍ MIGRACE NA WINDOWS AZURE	49
6.3	VYHODNOCENÍ MODELOVÝCH SITUACÍ A JEJICH MOŽNÁ ŘEŠENÍ	49
	ZÁVĚR.....	51
	SEZNAM POUŽITÉ LITERATURY	53
	SEZNAM OBRÁZKŮ	57
	SEZNAM TABULEK.....	58
	SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK	59
	SEZNAM PŘÍLOH.....	60

ÚVOD

V současné době globalizovaného propojeného světa, kde internet je všudypřítomný a propojení lidí prostřednictvím něj a jeho využitelnost je dalekosáhlá, je situace s ukončením podpory v současnosti nejrozšířenějšího operačního systému Windows 10 palčivým problémem. Již dávno nejsme v době jediného zařízení, jež je schopno se připojit k internetové síti, potažmo na tomto zařízení konat všechny možné činnosti. Tímto zařízením byl v minulosti a po masovém rozšíření PC IBM právě osobní počítač, kdy tyto po nástupu sofistikovanějších operačních systémů s uživatelsky přívětivým grafickým rozhraním ovládl právě operační systém společnosti Microsoft nazvaný příznačně Windows, dle schematicnosti, jenž se tento systém ovládal, tedy prostřednictvím čtvercových obrazců tedy „oken“. Díky následnému rozmachu a propojitelnosti počítačů prostřednictvím sítě Internet dosáhl globálního přesahu, je obsažen na doslova miliardách zařízení a stanic, jež ovládají běžní uživatelé, je zastoupen ve státní sektoru, soukromém sektoru až po systémy kritické infrastruktury jednotlivých států. Z toho důvodu jest ukončení jeho podpory v souvislosti s udržením kyberbezpečnosti na daných zařízeních, taktéž otázkou, jež má přesah do Ochrany Obyvatelstva. V rámci této práce jsou definovány hrozby, jež mohou souviset s během a používáním neaktualizované verze Windows na osobních počítačích. Jednoznačně je zde prezentováno, že podcenění tohoto problému je hrozbou jak pro jednotlivce, tak i pro skupiny, malé i větší firmy, organizace, aparát státní správy a samosprávy až po tolik diskutované a časté terče kybernetických útoků, což jsou subjekty kritické infrastruktury.

Cílem této práce je komplexní popis dané problematiky, poukázání na možnosti řešení a v neposlední řadě doporučení jak k celé situaci s ukončením podpory Windows 10 přistoupit a nepodcenit tento dožijící se vážný kyberbezpečnostní problém. V průběhu praktické části práce jsou dále k tomuto účelu využity vědecká metoda komparace, k zjištění aktuálního stavu byl dále proveden strukturovaný rozhovor a dále byli použity metoda ekonomického modelování s analýzou nákladů, případně uvedení doporučení a kritické zhodnocení jednotlivých možných řešení.

I. TEORETICKÁ ČÁST

1 VÝVOJ OPERAČNÍHO SYSTÉMU WINDOWS

Kam míříme a kam spějeme je jedna s pradávných otázek lidstva. Co se týká vývoje samotného operačního systému Windows ani tento nepřišel z ničeho, ale jeho současný status je dědictvím jistého vývoje a ač je častokrát označován jako operační systém pro konzervativní zákazníky, prožil si jistou katarzi v řádech desítek let. Tento úspěšný vývoj s někde trnitější cestou mu v současné době vydobyl nezastupitelnou roli vně osobních počítačů jako jejich nezpochybnitelná softwarová součást.

Obšírněji se v této části jest věnováno jednotlivým verzím Windows, kdy následně v textu je představen Windows 11 jako logického následovatel ze stejné rodiny tohoto produktu, jež sebou nese jistá specifika a zvláštnosti oproti svému generačnímu předchůdci.

1.1 Společnost Microsoft

Století 21. je mnohými označováno jako věk skutečně a popravdě elektronický, kdy většina našeho času a vnímání se přesouvá právě do virtuálního světa, jenž je samozřejmě částečně a neodmyslitelně propojen se světem reálným, nicméně i přesto jako takový existuje ve své podstatě v základu pouze v binárních soustavách, komplikovaných kódech a algoritmech, kdy ho může vnímat prostřednictvím zobrazovacího zařízení v našem případě nejčastěji PC (personal computer).

Firma Microsoft je v současní chvíli, tedy při tvorbě této práce (počátek roku 2025) považován dle publikovaných žebříčku Forbes mezi celosvětově 5 nejhodnotnějších firem, kdy hodnota značky je v danou chvíli odhadována na 461.1 MLD USD (CHIP 2025). Pakliže bychom se bavili o hodnotě firmy jako takové v průběhu času samozřejmě může její hodnota nabývat i klesat, nicméně je důležité k tomuto dodat, že hodnota firmy Microsoft je stabilní v průběhu několika minulých desetiletí, kdy od 90. let minulého století si drží tento status.

Firmy jako takové nerostou sami od sebe, ale za jejím růstem stojí především stabilní a silný produkt. Pomyslným zlatým grálem výrobních produktů je subjekt, jenž bude globálně rozšířen do stovky či miliard domácností. Tímto produktem pro firmu Microsoft byl operační systém Windows. Dalo by se říci jak vzrůstalo zastoupení a významnost tohoto operačního systému v počítačích vzrůstala tak i hodnota a velikosti firmy Microsoft. Ač v současné době to již nedějí v portfolii produktů nabízené touto firmou jako jediný subjekt, i dnes má v jejím zastoupení klíčovou roli a přestože firma Microsoft dále se rozvíjí na trhu s cloudovými službami (AZURE), vyvíjí již dlouhá desetiletí kancelářský balík pevně spjat

s Windows tedy OFFICE v současné době označený jako 365 a má nepopíratelné investice na poli umělé inteligence, je operační systém Windows nadále majoritou v jeho portfoliu.

1.2 Počátky společnosti Microsoft

Firma Microsoft byla dle dostupných zdrojů založena dne 4.4.1975 zakladateli Billem Gatesem a Paulem Allenem. Sídlo jako takové má v americkém státě Washington konkrétně ve městě Redmond. (SUTURI 2025)

Prvním vyvinutý operačním systémem touto společností ještě nebyl operační systém Windows, ale jednalo se operační systém MS – DOS, kdy následně až v roce 1985 byla vydána první verze operačního systému Windows verze 1.01 Tato sama o sobě byla pouze jakousi sběrnici mnoha daných aplikací pouze s omezenými funkcemi. (Microsoft, 2025).

Co vůbec vedlo k prvotnímu rozkvětu operačního systému Windows bude nyní vysvětleno trochu obšírněji, protože je to zajímavá, i když dnes již lehce pozapomenutá etapa vývoje. Jež před příchodem první verze Windows 1.01 se společnost Microsoft inspirovala v té době u populární firmy Xerox, kdy v jejich laboratořích se v danou dobu, tedy počátkem 80. let minulého století vyvíjel operační systém na bázi oken s lištovými nabídkami a ikonami. O tento systém, respektive o nápady tohoto systému měl zájem taktéž v té době populární firma Apple. Zástupci této společnosti Steve Jobs a Steve Wozniak navštívili dané laboratoře, kdy se v daném systému taktéž inspirovali. Z tohoto byl následně odvozen produkt společnosti Apple, jež přišel na trh krátce na to. Jednalo se o kompaktní počítač Apple Macintosh, jež jako první přišel se skutečným využitím „okenních“ systému, kdy tyto dále obohatil o další nezbytnou periférii, a to je myš. Dalo by se říci, že zároveň s ním byl uvedena první verze operačního systému Windows. (zive , 2004)

Tento dnes již zapomenutý spor, kdy jednotlivé společnosti tedy Apple a Microsoft se v danou chvíli obviňovali z toho kdo komu ukradl daný operační systém, jsou již v dnešní době zapomenuty, ale s největší pravděpodobností se ony s větší částí inspirovali u společnosti Xerox a návrhu jejich řešení.

I přesto, že využitelnost první vyšlé verze operačního systému Windows mohla být lehce sporná, byl to ve své podstatě jen z neoddiskutovatelných stavebních kamenu dalších verzí, kdy jistě zavedené standardy následně vydrželi po mnoho dalších let.

1.3 Windows a jeho jednotlivé verze

Jak bylo uvedeno, Windows je tedy operační systém, a to již v historii mnoha let dominující v segmentu osobních počítačů. Důležitý a podstatný je hlavně z toho důvodu, že se masově rozšířil všude, kde jen to šlo. Důvod proč se takto stalo je především marketingová politika spojená s revolučním využití periférií počítačů, kdy dále k tomuto dodal Microsoft vhodnou širokou softwarovou výbavu.

Rámcově bylo v minulých odstavcích zaměřeno obšírněji na představení společnosti Microsoft, jež stojí za operačním systémem Windows. V této části bude rozebráno jednotlivé historické verze operačního systému až po současnosti, kdy dále bude rozebírány rozdíly mezi různými druhy distribucí. Protože ve své podstatě není Windows jako Windows.

V jednoduché tabulce níže si popisuje vydání jednotlivých verzí Windows, kdy popsání jednotlivých dopadů vydaných verzí na segment osobních počítačů by mohl vydat na samostatnou práci, popřípadě knihu. Nicméně ty základní si uvedeme níže, kdy v závorce za nimi se nachází rok vydání:

- Windows 1.01 (1985)
- Windows 1.03 (1986)
- Windows 2.0 (1987)
- Windows 2.1 (1987)
- Windows 3.0 (1990)
- Windows 3.1 (1992)
- Windows NT 3.1 (1993) – první 32bitový systém
- Windows 3.51 (1993) – finální verze první etapy vývoje
- Windows 95 (1995)
- Windows NT 4.0 (1996)
- Windows 98 SE (1999)
- Windows ME (2000)
- Windows 2000 (2000)
- Windows XP (2001)

- Windows Server 2003 (2003)
- Windows Vista (2007)
- Windows 7 (2009)
- Windows 8 (2012)
- Windows 8.1 (2013)
- Windows 10 (2015)
- Windows 11 (2021)

Nutno pro celkový nástin ještě poznamenat, že především poslední dvě verze Windows jsou ještě interně rozdělovány prostřednictvím verzí nahraného update pomocí aplikace Windows update.

Pro komplexní informace je dobré definovat a pro případ vysvětlení věcí následujících v této práci, kdy byla ukončena oficiální podpora několika posledních významných verzí distribucí významných verzí

- Windows 7 – 14.1.2020
- Windows 8 – 12.1.2016
- Windows 8.1. – 9.1.2018
- Windows 10 – 14.10.2025

V práci nejpodstatněji je definováno ukončení podpory v současné době stále nejpoblárnějšího a zřejmě i nejzastoupenějšího operačního systému tedy Windows 10. Dle oficiálních stránek firmy Microsoft k tomuto má dojít dne 14.10.2025 (Microsoft 2025). Z daného uvedeného je jasné patrné, že podpora Windows 10 jako taková, je společností Microsoft poskytována po dobu 10 let. Na délku podpory, jež povětšinou Microsoft takto nabízí a poskytuje je často odvislá od komerční úspěšnosti daného systému. Ne nadarmo je to operační systém s druhou nejdelší dobou oficiální podpory, kdy po delší dobu byl podporovaný jen Windows 7.

Co se týká samotného možného pokračovatele distribucí z rodiny společnosti Microsoft tedy Windows 11, ten se v současné době nabízí v těchto uvedených distribucích:

- Windows 11 HOME

- Windows 11 PRO
- Windows 11 PRO SEDUCTION
- Windows 11 SE
- Windows 11 PRO FORK WORSKATION
- Windows 11 ENTEPRISE
- Windows 11 EDUCATION
- Windows 11 MIXED REALITY

Co se týká jednotlivých verzí jsou tyto mnohdy rozdílné jen určitými specifickostmi užitého systému či periferie. Jediný větší rozdíl lze spatřovat v distribuci nazvané ENTEPRISE. Tato konkrétní je především zaměřena na zákazníky s multilicenční smlouvou, obsahuje technologie, jež jsou povětšinou použity ve větších firemních prostředí. (Klatovský 2022).

1.4 Minimální systémové nároky Windows 11

Další důležitým specifikem, jež její důsledky budou rozebíraný především v praktické části je hardwarová náročnost dnes aktuálního operačního systému Windows 11. V dobách minulý bylo pravidlo, jemuž se říkalo Moorův zákon. Tento v roce 1965 definoval Gordon Moore. Jednalo se osobnost, jenž byla v 70. letech jako spoluzakladatel firmy Intel. Tento v roce 1965 prohlásil, že v průběhu 12 po sobě jdoucích měsíců se počet transistorů zdvojnásobí. O několik let později v roce 1975 tento zákon upravil na již i dnes známé rčení, že v průběhu 24 měsíců se výkon počítačů zdvojnásobí (svethardware 2024). K úplnosti daného nutno poznamenat, že tento minimálně v tomto a posledním desetiletí nepsaná platný zákon již lehce zastaral, a jeho faktická platnost je dnes narušena tím, že hrubý výkon jako takový se nebere momentálně až takto v potaz, kdy jeho nárůst v poslední době již není dvojnásobný ale pouze poměrný.

Současné hardwarová specifika hlavní pokračovatele operačního systému Microsoftu tedy jeho verze s označení 11 jsou dle oficiálních stránek níže uvedeny jako:

- 64bitový procesor o taktu min 1 GHz se dvěma či více jádry
- 4 GB RAM
- 64 GB úložiště

- Rozhraní UEFI
- TPM ve verzi 2.0
- Kompatibilní DirectX 12 grafická karta
- Obrazovka s rozlišením alespoň 720 p

(Microsoft.com, 2025)

S výkonem výpočetní techniky jde v ruku v ruce i hardwarová náročnost daných aplikací, programů, operačních systémů. I když vývoj „hrubého“ výkonu v posledním desetiletí zvolnil, kdy se větší důraz klade na specifické použité technologie, stále tento trvá. Jeden z aspektů nového operačního systému Windows 11 je jeho zvýšená hardwarová náročnost, kdy nutno poznamenat že málokdy v minulosti bylo v průběhu změny operačního systému zvolit ráznější upgrade. Celá situace lze ale nutno vnímat v kontextu doby, kdy problematika přechodu na nový operační systém skýtala vždy mnohé nové výzvy. V minulosti docházelo tudíž často k upgradování hardwarových součástí počítačů z důvodu již výše popsaného Moorova zákona, kdy tomuto častokrát odpovídal i vývoj odpovídajícího hardwaru. Jelikož vývoj v posledních letech je spíše pozvolnějšího charakteru, může se stát hardwarová náročnost pro tradičně konzervativní zákazníky částečně problematická, jelikož tito nejsou ostatními okolnostmi do hardwarového upgradu takto nepřímým tlakem.

1.4.1 TPM 2.0

V horizontu posledních minimálně 5 až 8 let jsou různými výrobci na současné základní desky přidávány moduly TPM 2.0. Jelikož dané výhody využití a zvýšení zabezpečení jsou natolik zásadní, tak bylo rozhodnuto o nutnosti jeho implementace do Windows 11 a je to jeden z hlavních rozdílů oproti jeho předchozí verzi, kde tato implementace chyběla.

Čip TPM jako takový funguje na principu zabezpečeného úložiště citlivých dat a taktéž jako modul pro ověření integrity. Hlavními funkcemi Trusted Platform Module, jež je jeho celý název jsou tyto:

- **Slouží jako úložiště šifrovaných klíčů:** pomocí nástroje nazývaného Bitlocker šifruje data na harddisku takovým způsobem, aby nedošlo k jejich zneužití třetí stranou

- Securete boot : během bootování systému zabraňuje nechtěným aplikacím (malware) spuštění na pozadí. Tohoto docílí prostřednictvím ověření platnosti ovladačů operačního systému současně s ověřením integrity a správnosti operačního systému a také ověření neautorizovaných spuštěných programů v paměti.
- Windows Hello : tento nástroj slouží pro ukládání unikátních biometrických dat uživatele a zabraňuje jejich zneužití
- Šifrování dat : pomocí generování náhodných čísel a krypto operací dále zlepšuje bezpečnost, také sleduje při spuštění přítomnost dílčích rootkitů, jež by snad tento proces při autorizování systému mohli odhalit

(dell.cz,2025)

1.4.2 Podporované architektury procesorů

Pakliže bylo v předchozím odstavci utvořen prostor věnování se modulům TMP 2.0 je dále nutné se zmínit i o dalších hardwarových nárocích systému Windows 11. Z důvodu vyšších požadavků udávaných společností Microsoft i v tomto atributu došlo ke zvýšení požadavků. Co se týká podporovaných procesorů, tyto lze najít na samotných webových stránkách společnosti Microsoft . (microsoft.com,2025)

Předně jak už bylo výše uvedeno jedná se tedy pouze o 64bitové procesory. Kromě tohoto jsou nicméně zmíněny i další nároky. Podporovány jsou především tři série procesorů a to

- Intel CORE
- AMD Ryzen
- Qualcomm – Snapdragon

Co se týče konkrétních typů tak procesory Intel jsou podporovány od konkrétně generace 8., kdy procesory nesly kódové označení Coffe Lake (rok 2017)

Dále co se týče procesorů AMD ty jsou podporované až od 2. generace, konkrétně od architektury ZEN + (rok 2019) spolu ještě s některými procesory z rodiny Athlon a Threadripper od série 2000

Dále od společnosti Qualcomm jsou podporované procesory typu Snapdragon X plus a X ELITE.

Důvodu proč tomuto tak je lze hledat opět ve zvýšené bezpečnosti. S každou další novou generací procesorů, tyto v architektuře obsahují nové sady instrukcí. Jedná se především o instrukce MBEC (MODE – BASE Execution control) a POPCNT (počítadlo bitů).

Nutno říci že důvod proč se v této části více zabírat konkrétními specifiky HW nároků je takové, že při uvedení současné verze Windows 11 na trh, dané HW nároky budili jisté kontroverze. Důvody kromě zřejmých pro – ekonomických jsou ale i především bezpečnostní. Všechny dané novější technologie spolu s pravidelnými aktualizacemi poskytují nejvyšší možnou ochranu, jež mohou v současné době osobní počítače poskytovat. Proto se v další část, věnuje se právě aktualizacím.

1.5 Windows update

Aktualizace. Slovo dnes tak známe a hojně používané v jakémkoliv IT oboru. Dříve tomu ovšem tak nebylo. Dnes se často skloňuje v rámci kyberbezpečnosti to, že systém musí být včas a vhodně zabezpečený, aktualizovaný na poslední verzi, jen při takovém používání daného software se můžeme cítit uživatel náležitě bezpečný.

Samozřejmě toto nese právě rozšiřitelnost internetového prostředí. Proto není divu, že co se týče produktů společnosti Microsoft, samotná možnost aktualizací se objevila v nich až s Windows 98.

Je dobré si v danou chvíli udělat malý exkurz do minulosti. Windows 98 byl v dané době revoluční v mnoha ohledech a jeden z nich byli právě zmíněné aktualizace. Už v té době se jednalo o jisté bezpečnostní záplaty. Samotný automatizovaný proces nabídl nicméně až Windows XP, který tento postup zefektivnil a pro uživatele taktéž zjednodušil. Následující operační systém s značením Vista pak přidal možnost aktualizací nejen operačního systému ale taktéž předlužených programů pochopitelně z rodiny firmy Microsoft. Nicméně až Windows 10 přichází se samotným systémem, komplexním. V době svého uvedení byli totiž Windows 10 často označovány jako poslední systém, a přetvoření jeho funkčnosti do systému vedeném jako služba. Jak už dnes dobře známo Windows 10 poslední verzí operačního systému od Redmondské firmy nebyl a je jistý předpoklad, že jím nebude ani jejich nejnovější počín nesoucí kódové označení Windows 11.

Princip celého zavedení systému Windows Update se váže na skutečnost, kdy v době vydání daného softwaru nejsou známi veškeré bezpečnostní chyby, jež tento může obsahovat. Povětšinou se na tyto přijde tedy až post. Z daného důvodu je pro zaručení bezpečnostní nutné v co nejkratším časovém intervalu tyto aktualizace, a tedy bezpečnostní záplaty nainstalovat a dané chyby tím opravit. Kromě oprav samotných chyb nicméně dochází taktéž k rozšíření a zdokonalení dalších funkcí systému. Taktéž jeden z důvodů, proč se musí aktualizace vydávat je upravení či uzpůsobení softwaru nově vydanému hardware (Pecinovsky 2020).

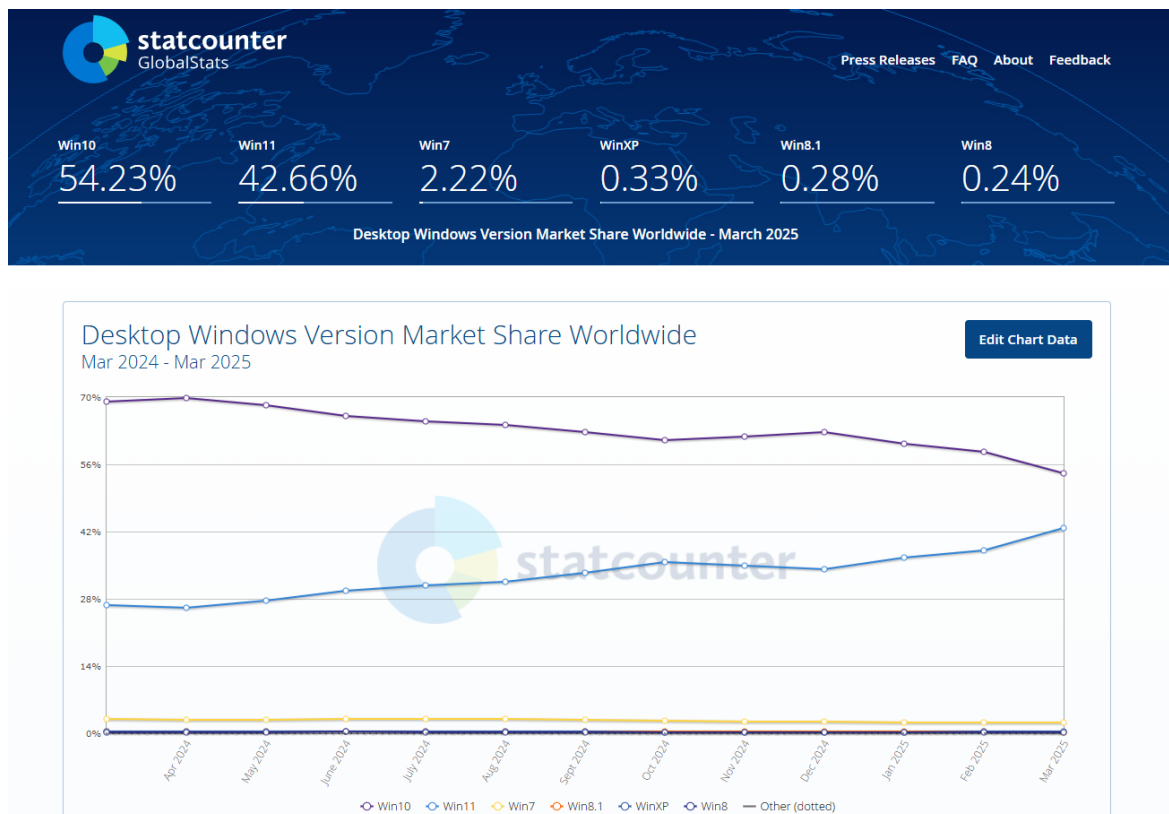
V neposlední řadě je dobré uvést, že při posuzování hrozeb související s ukončením podpory Windows 10 je nutné i pochopit základní mechaniky systému. Systémová bezpečnost totiž vychází z architektury jádra Windows NT, už o této doby je jasná zranitelnost, pakliže absentuje pravidelnosti aktualizací. Riziko je především zneužití zprávy paměti nebo přístupu k jádru systému (YOSIFOVICH et. All.,2017)

1.6 Rozšířenost OS MS Windows

Statistiku zastoupení operačního systému Windows potažmo jeho jednotlivých verzí není úplně otázka, na niž lze získat jednoduchou odpověď. Celosvětově dle zjištění neexistuje webová doména, případně jiná veřejná prezentace, kde by mohlo být s ohledem na vyšší procenta určen přesný přehled zastoupení operačního systému Windows.

Pakliže ve věci bude pracováno s jistou mírou odchylky, jež je pro tuto práci a prezentace výsledků dostatečná, lze najít web zabývající se takovýmito statistikami. Jedná se o web Statcounter.com. Pakliže bereme v potaz všechny dostupná zařízení včetně mobilních telefonů a tabletů, lze se dopátrat že k března roku 2025 zastupuje operační systém Windows asi 25 % zastoupení na všech elektronických zařízeních pracujících pod nějakým operačním systémem. (statcounter.com)

Další zajímavější statistikou je již zastoupení jednotlivých operačních systémů. Dle realizovaných statistik Windows 10 obsahuje asi 54 % zařízení na celém světě, kdy Windows 11 obsahuje asi 42 %. Co je tedy ještě dále zajímavější, že zbylá 3 procenta jsou starší verze operačních systémů Windows, jež jsou již léta nepodporovaná aktualizacemi a bezpečnostními záplatami. K celé statistice je ještě dobré se vyjádřit takovýmto způsobem, že toto zajišťuje společnost StatCounter Ltd sídlící v hlavním městě Irsko Dublinu, kdy společnost byla založena roku 1999. Servery sbírají analytická data z ohromného množství webových stránek. (statcounter.com)



Obr. 1 statistika zastoupení OS Microsoft Windows (STATCOUNTER, 2025)

S definovaných hodnot grafu lze taktéž vysledovat že zastoupení operačního systému Windows 10 pozvolna klesá, nicméně vzhledem k okolnostem a blížícímu se oficiálnímu konci jeho podpory, tak nicméně ne až tak drastickým tempem.

2 ASPEKTY KYBERBEZPEČNOSTI

V první kapitole byli představeny počátky vývoje operačního systému Windows, potažmo byl definován současný stav, a tedy rozšířenost operačního systému Windows včetně jeho verze s číslovkou 10. Další text bude zaměřen na kyberbezpečnost jako takovou.

Pakliže je brán operační systém jako prostředí, v němž uživatel pracuje a uchovává zde mnohdy citlivá data, lze toto taktéž chápat jako kybernetický dům. Jako skutečný dům musí mít i tento jisté vrstvy opatření, jež pomohou zvýšit jeho odolnost případně minimalizovat případné hrozby, jež sebou nese nebezpečné prostředí internetu. Důležitým kritériem pro možné ohrožení kybernetických dat, identit a dále, je samotná přítomnost v online světě. Jednoduše vzato v momentě, kdy je uživatel v tak zvaném off-line módu vše co si je zde uvedeno neplatí. Nicméně neplatí taktéž přenos dat mezi jednotlivými počítači, sdílení, odezva a věci jež po většinou je to to hlavní co od osobního počítače čekáme a je to nezbytnou součástí současné efektivní práce s nimi. Je nadále potřeba zmínit, že povětšinou ty hlavní hrozby a prostředky obrany jsou zmíněny především v momentě, když je zároveň zařízení připojené k síti internetu.

Dále je třeba uvést, že hrozeb jako takových je v cyber světě spousty, nicméně ne všechny mají důvodnou souvislost s ukončení podpory Windows 10, potažmo s ochranou obyvatelstva. Dle těchto specifik je i tato část zaměřena na pravidla a rizika související přímo s ukončení podpory Windows 10.

2.1 Pravidla Kyberbezpečnosti

Aby byla udržena aktivita uživatele v online světě bezpečnou, je nutné dodržovat alespoň elementární pravidla v pohybu v tomto světě. Základními pravidly kyberbezpečnosti tedy jsou:

- Nutnost užití dostatečně silných hesel
- V ideálním případě dvoufázové ověření při přihlášení
- Záloha klíčových dat
- Obezřetnost související s otevřením podezřelých emailů či jejich příloh
- **Nutnost udržení si aktuální verze operačního systému stejně tak i programů**

Z daného je patrné, že věci, jež můžou být nějakým způsobem ovlivněny se týkají osobní vlastní disciplíny či řekněme jisté dávky obezřetnosti. Co by měla být brána ovšem jako samozřejmost je udržování aktuálnosti operačního systému potažmo nainstalovaných a používaných programů. (legislativa.cz)

2.2 Problematika udržení software v aktuální verzi

Udržení aktuální verze operačního systému společně s aktualizovanými verzemi používaných programů, potažmo i ovladačů je hlavním aspektem kyberbezpečnosti. Taktéž se jedná o jeden z aspektů, jenž je velice často podceňován. V obecné rovině lze chápat, že příčiny prolomení zabezpečení může být v té nejjednodušší formě:

- Vědomé
- Nevědomé

Vědomé prolomení bezpečnosti je situace, kdy danému útočníkovi předávám ve své podstatě klíče a dále mu dávám návod, jak mě oklamat a citlivý data odcizit. Jedná se například útoky typu phishing, kdy jsou předávány citlivé údaje kreditních karet. I když se jedná v danou chvíli samozřejmě o uvedení v omyl a převážně o podvodné jednání, pakliže v danou chvíli budu dodržovat i jistou míru obezřetnosti nemůže k ničemu takovému dojít, případně minimalizují riziko takového incidentu. Opačná situace je ovšem u nevědomého prolomení bezpečnosti. V danou chvíli osoba, ač skutečně živá entita na druhém konci připojení či nějaký automatizovaný software v daný moment a chvíli využije bezpečnostních rizik, děr, jež takovéto mohli právě vzniknout na používané stanici v souvislosti s ne aktualizací daného operačního systému. (Coxe,2019).

Nutno ještě poznamenat, že v rámci cíleného kybernetického útoku se pachatel zaměřuje přímo na konkrétní objekt, kdežto v rámci plošného kybernetického útoku pachateli nezáleží na tom, kdo se přesně stane jeho obětí. V této parafrázi by se dalo říci, že útoky na neaktuální verze jsou povětšinou cílené, ale můžou být taktéž i plošné. (Šulc, 2018).

2.3 Druhy kybernetických hrozeb

Kybernetická hrozby související s neaktuální verzí Windows jsou nemalá. Nicméně je třeba připomenout, že míra rizika či míra připravenosti či lépe řečeno nepřipravenosti uživatelů může být různě odstupňovaná. Dále je třeba si říci, že pro udržení bezpečnosti a vyvarování se hrozeb nestačí pouze mít aktuální verzi software operačního systému, ale

taktéž je nutné udržovat aktuální verze i samotných programů na něm spuštěných. Oproti minulosti určitě došlo k omezení počtu běžně nainstalovaných programů, kdy hodně samotné činnosti je orientováno do online služeb a cloudu, nicméně i na toto bychom neměli zapomínat. Dalším aspektem, jež může taktéž ovlivnit možnost kybernetického ohrožení je neaktuální verze softwarových ovladačů ani na toto by se nemělo zapomínat.

K samotným kybernetickým útokům, jež můžou přijít v momentě, kdy si nesplníme nutná bezpečnostní opatření může být tyto typy útoků :

- Malware útok
- Ransomware útok
- Phising útok
- Worm útok
- Rootkit

Jednotlivé kybernetické útoky bude dále rozebrány a na konkrétních případových studiích ukázaný jejich následky.

2.3.1 Malware

Běžný typ kybernetického útoku formou škodlivého software. Společným cílem daného typu útoku je získání informací, popřípadě krádež identity, špionáž a narušení služeb (Sedlák, Konečný a kolektiv, 2021)

Malware je ve své podstatě označení pro jakýkoliv program, jež může způsobit škody na zařízení a dle specifík útoku se pak může rozdělat na další podmnožiny. V počítačích, jež nejsou pravidelně aktualizované povětšinou objeví skrytou chybu, jež tato aktualizace by případně ošetřila, kdy dále může získat přístup k samotnému systému.

2.3.2 Ransomware

Jedná se malware, jež má schopnost infikovat zařízení zranitelných cílů a následně zde se získanými daty různými způsoby vydírá zprostředkovatele či majitele zařízení, na než byli tyto data uloženy (Sedlák, Konečný a kolektiv, 2021)

Útoky jako takové můžou mířit především na

- Státní sektor

- Zdravotnická zařízení
- Kritickou infrastrukturu
- Výrobní podniky

Opět v zařízení, jež není aktuální může dle bezpečnostní chyby objevit možný přístup a dále pokračuje podle předem daného scénáře odcizení dat a následně vydíráním.

2.3.3 Phising

Jedná se útoky, jež využívají sociální inženýrství ke krádeži uživatelských dat, tedy jedná se o přihlašovací či platební údaje. Díky těmto podvrhům lze získat přístup a zneužít například přístup do mailu případně i do cloudové služby pomocí podvržených DNS a certifikátů (Sedlák, Konečný a kolektiv, 2021).

Phising ve své podstatě útočí na uživatele psychologicky, kdy tento následně dobrovolně či nevědomky sdělí útočníkům klíčové přihlašovací údaje. Neaktualizovaný software má v danou chvíli v tomto roli ve smyslu případného otevření stránky, jež by byla za normálních okolností blokována Windows Defenderem, při přesahu do softwaru taktéž prohlížeče neaktualizované na neaktualizovaném software můžou taktéž otevřít stránky či přílohy, jež by záplatami byli jinak blokovány.

2.3.4 Worm útok

Worm, česky červy, patří do skupiny malware. Na rozdíl ovšem od klasických virů se šíří automaticky bez nutnosti propojení s programem. Při svém šíření a množení mnohdy využívá právě chyby v bezpečnosti operačního systému, jež jsou pravidelnými aktualizacemi opraveny.

Při malém exkurzi do historie si můžeme uvést, že první červ jež byl vytvořen vznikl studentem Cornellovy univerzity Robertem Morrisem. Říkalo se mu tak zvaně Morrisův červ. Jednalo se o rok 1988, proto se není čemu divit, že vyřadil asi 10% všech zařízení připojených k tehdejší síti Internet. (Kolouch, 2019).

2.3.5 Rootkit

Jedná se o škodlivý kód, jež umožňuje útočníkovi získání přístupu k celému systému a tím v konečném důsledku jeho ovládnutí. Většinou se vydávají za systémové procesy,

soubory a složky, případně registry. Z daného důvodu je velmi složitá jejich detekce a jejich případné odstranění. (eset,2025)

Rootkity při svých zákeřných útocích opět využívají bezpečnostních slabin a nedostatečných aktualizací Windows. Z daného popisu lze odvodit, že následky tohoto škodlivého kódu mohou být devastující.

3 PLATNÁ LEGISLATIVA V ČR, EU, SVĚTĚ

V rámci této bakalářské práce byla představen samotný předmětný software Windows potažmo jeho vývoj, dále teoretická hrozby kyberbezpečnosti související s nebezpečím užívání neaktuálního operačního systému, v třetí části si rozebereme platnou legislativu, jež nepřímo ovlivňuje a zajišťuje dodržování kyberbezpečnosti, řeší případné sankce a nastoluje i jiné standardy.

Z výše zmíněného vyplývá, že užití neaktualizovaných Windows může znamenat výrazné bezpečnostní riziko při jejich užívání, pro naše účely se zaměříme na legislativní rámec v rámci České republiky, Evropské Unie a zbytku světa.

3.1 Legislativa v České republice

V rámci České republiky je stanoven právní rámec zákonem č. 181/2014 Sb. o kybernetické bezpečnosti. Zákon jako takový nezakládá trestně právní odpovědnost pachatelů kybernetických útoků, toto řeší až trestní zákoník 40/2009 Sb. nicméně vytváří systém bezpečnostních opatření jež mají výskytu kybernetických bezpečnostních incidentů předcházet. Nad tímto drží dohled Národní úřad pro kybernetickou a informační bezpečnost. (Kolouch,2019).

Zákon jako takový obsahuje i v jednotlivých paragrafech sankce pro instituce kritické infrastruktury, jež jsou povinni dodržovat pravidla kybernetické bezpečnosti, kdy jedním z nich je samozřejmě udržování aktuálních verzí operačního systémů potažmo programů.

3.2 Legislativa v Evropské Unii

V rámci Evropské Unie byla přijata směrnice NIS, jež přijal Evropský parlament dne 6. července 2016 k zajištění vysoké úrovně bezpečnostních sítí a informačních systémů v EU. Směrnice dále prošla revizí v roce 2020 s návrhem směrnice NIS 2 (Directive (EU) 2022/2555). Návrh směrnice NIS 2 především v rámci kyberbezpečnosti zpřísňuje minimální bezpečnostní opatření. K dodržování platnosti směrnice byla již v minulosti vytvořena agentura ENISA (Kolouch,2019).

Platná legislativa EU přímo nutí odpovědné instituce v ní vyjmenované k ošetření rizika souvisejícího s ukončení podpory aktuální verze Windows 10 a nalezení řešení tak aby se dostatečně snížila možnost kybernetického ohrožení. Nezajištěná data a jejich případný únik taktéž řeší v rámci Evropské unie směrnice GDPR

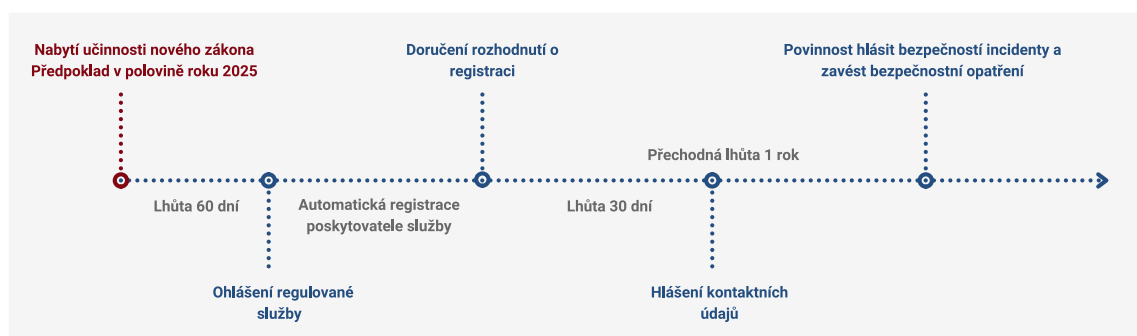
3.3 Legislativa ve světě

V rámci zemích mimo Evropské unie, pro západní svět blízké, tedy třeba ve Velké Británii, vzhledem ke kontextu minulých let a přítomnosti v Evropské unii tato využívá taktéž části směrnice NIS. Oproti tomu v USA v rámci kybernetické bezpečnosti je využíván zákon označen zkráceně FISMA.

System jako takový rozlišuje úrovně bezpečnosti, dle rozdílného zařazení ovládacích zařízení na 5 tříd, kdy stejně jak evropské směrnice požaduje po vládních agenturách či součástech kritické infrastruktury dodržování daných bezpečnostních standardů. (cisa.gov, 2025) .

3.4 NIS 2 Aplikování směrnice v Českém právu

V rámci vypíchnutí toho nejdůležitějšího je dobré si rozebrat dále v samostatné části směrnici NIS 2 jinak tedy Directive (EU) 2022/2555). Jedná se o nejdůležitější Evropskou směrnici vydanou v poslední době, kdy její aplikace bude nutná i do českého práva. V platnost směrnice jako taková vstoupila v roce 2023, kdy se v následujícím blízkém období čeká implementace do českého práva. Implementaci jako takovou zajišťuje v České republice NÚKIB, což znamená tedy Národní úřad pro kybernetickou a informační bezpečnost, tento taktéž odpovídá za celou transpozici. (delouite.com, 2025)



Obr. 2 Harmonogram zavádění zákona (NUKIB, 2025).

Platnost novely je tedy momentálně odhadovaná na polovinu roku 2025, kdy její princip je, že dopadne na daleko více organizací a subjektů než poslední právní úprava. Tyto organizace a subjekty budou muset nově řešit především:

- Přísnější dohled NÚKIB (včetně auditů u firem, organizací) z toho plynoucí vyšší možné sankce a pokuty

- Přísnější požadavky na kyberbezpečnost (nutnost zavedení bezpečnostní opatření, řízení rizik, dvojfázových ověření ...)
- Povinnost posoudit softwarový dodavatelský řetězec (týká se tedy software třetích stran)

V době dokončení práce byl návrh zákona dne 25. dubna 2024 schválen Poslaneckou sněmovnou Parlamentu ČR, kdy nyní schází pouze projednání v rámci Senátu. (NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST, 2025)

II. PRAKTICKÁ ČÁST

4 HROZBY A HISTORICKÉ PARALELI

V teoretické části byli definovány základy probírané problematiky. Byl vyhodnocen především historický vývoje operačního systému společnosti Microsoft, důvody jeho rozšíření, časovou posloupnost vydaných verzí a jiné. Dále byla uvedena možná bezpečnostní rizika v teoretické rovině, jež jsou hrozbou pro uživatele a firmy, tedy pro koncové zákazníky. V neposlední řadě byla uvedena i právní opora v rámci boje proti kyberkriminalitě a pravidla kyberbezpečnosti, jež je potřeba důsledně dodržovat, abych v co největší míře regulovali případná rizika.

Další část a úvodní část praktické práce bude zaměřena na historické paralely, jež jsou v přímé souvislosti s možným ukončením podpory operačního systému Windows. Prvotně budou prezentovány případové studie, kdy bude rozebíráno jednotlivé vybrané případy a tyto následně metodou komparace analyzovány. Pro pochopení celé problematiky je nutno poukázat na skutečné situace a dopady, jež z takových událostí vyplynuly. Skutečnosti s těmito incidenty souvisejícími dále budou porovnány se současným stavem se zamyšlením, zda by jednou uskutečněnému mohlo k nim opětovně dojít.

Z pohledu praktického bylo dříve vysvětleno, že pro udržení bezpečného pracovního prostoru ve svém zařízení je nutné dodržovat jisté bezpečnostní standarty. Pakliže toto dodrženo nebude, lze významnou mírou zvýšit riziko a potažmo i hrozbu případného útoku v následujících případových studiích si zanalyzujeme globální bezpečnostní incidenty, uvedeme, jaké měli následky v kontextu ochrany obyvatelstva a vyhodnotíme, jak lze tomuto předcházet případně se zamyslíme nad hypoteticky horší i lepší variantou v případě tohoto incidentu.

4.1 Případová studie WannaCry

V této případové studii bude zaměřeno na rozebrání systému příčin a následků, potažmo důležitosti napadení zařízení infekcí WannaCry a jakou souvislost má toto s historickou paralelou konce Windows 10.

WannaCry byl škodlivý kód typu Ransomware, jež zaútočil na počítače, na něž byl nainstalován operační systém společnosti Microsoft. K napadení počítačů došlo dne 12.5.2017. V rámci zařízení, jež byli napadeny se jedná o zhruba 300 000 systémů po celém světě, je zjištěno že se mělo jednat o systémy v 150 zemích světa, včetně systému kritické

infrastruktury. Jako zadní vrátka byl použit protokol SMB verze 1, jež pomáhá zařízení komunikovat s tiskárnou (avast.com,2025).

Analýzou bylo zjištěno, že infekce jako taková se skládá ze dvou částí. První je ve své podstatě červ, jež se dostane dovnitř systému a nakazí systémové soubory, má teda jakousi formu penetrace, kdy při tomto využije bezpečnostních slabín daného zařízení. V následujícím kroku šifruje dané soubory, kdy dále napadá základní spouštěcí systémové mechanismy. Následně uživateli předkládá tabulku s vyděračským zněním, ve které požaduje zaplacení dané částky, pakliže toto nebude splněno v následujících 3 dnech částku zdvojnásobí. Uživatel má taktéž znemožněn přístup ke svým datům díky zásahu této infekce. (AKBANOV et al, 2019)



Obr. 4 aktivní okno infekce WannaCry (VÍTEK, 2017)

Ve věstníku společnosti Microsoft byla tato bezpečnostní chyba, díky níž mohl původní červ infekce WannaCry vniknout do systému, odstraněna záplatou MS17-010. Microsoft tuto aktualizaci správně označil jako kritickou. Podstatné je, že tato aktualizace byla vypuštěna do systému Windows Update již, 14.3.2017. Z toho jasně vyplývá, že tato infekce cíleně útočila na systémy, jež právě neprochází pravidelnou aktualizací. Microsoft toto zmiňované označil jako chybu EternalBlue a dále označen jako CVE-2017-0144. Microsoft v danou dobu vydal následně zcela výjimečně taktéž aktualizace na v tou dobu již nepodporované operační systémy (Microsoft 2017)

Pakliže si situaci opětovně zanalyzujeme cílem útoku byli verze Windows od XP po Windows 8.1, včetně systému Windows 10, jež v daném období neprošel bezpečnostní aktualizací. V daném období, pakliže se vrátíme k teoretické části byli dle podpory společnosti Microsoft podporovány pouze systémy Windows 8.1. (jehož podpora končila 9.1.2018) a v té době nový systém Windows 10. Od uživatelů jako takových požadoval výkupné 300 USD.

Zastoupení a postavení operačního systému z té doby, lze najít například ve statistika statcounter.com. Z těchto vyplívá, že Windows 7 měl zastoupení 47 %, Windows 10 35 % a Windows 8.1 9 %. (statcounter.com,2017)

Pohled kontextu dané doby je třeba si připomenout, že Windows 7 byl velice populární a taktéž velice rozšířený systém. Po předchozí verzi Windows Vista nabízel spoustu uživatelsky přívětivějších vylepšení, běžel svižně i na starším hardware, jeho stínou stránkou bylo, že v době napadení viru WannaCry byl opětovně na ohromném množství počítačů, jelikož pakliže byli dodržována pravidla aktualizace operačního systému byl v bezpečí pouze systémy Windows 10 a Windows 8.1. v danou chvíli podporované. Lze namítnout, že Microsoft jako takový nabízel prodlouženou podporu pro operační systém Windows 7, nicméně z logiky věci lze soudit, že počet uživatelů, jež tuto placenou podporu realizuje je marginální v poměru ostatních uživatelů a jejich zařízení, jež se nachází bez podpory.

V kontextu Ochrany Obyvatelstva je nutno podotknout, že tento Ransomware útočil a napáchal škody na mnoha zařízení kritické infrastruktury z tohoto největší je zřejmě případ napadení počítačů Britské NHS (National Health Service).

Dle publikovaných studií je odhadovanou ztrátou pro britské zdravotnictví v částce 5,9 milionu liber. Ač během útoku jako takovém nebyla zapříčiněna smrt pacienta, bylo v celém systému neobsazeno na 13 500 lůžek. Dále byl kvůli nemožnosti využití elektronicky systému nutný přechod na papírovou dokumentaci. (GHAFUR et al., 2019).

Z tohoto aspektu lze jasně pozorovat, jak problematické je nedostatečná úroveň zabezpečení, kdy nutno poznamenat že britské zdravotnictví platí za dlouhodobě podfinancovaný sektor řekněme i ve světovém měřítku. Dále to jasně ukazuje nutnost pravidelných aktualizací softwaru a vytvoření plánu pro reakci na kybernetické incidenty. V opačném případě je v takovýchto případech snadné ohrozit prvky kritické infrastruktury, jež budou mezi cíli útočníků jedni z těch nejlukrativnějších.

4.2 Případová studia NotPetya

Druhou případovou studií s ještě destruktivnějšími dosahy je studie virové infekce malware NotPetya. Co se týče globálního dopadu, bude ukázáno na časové ose přibližná rychlost jeho šíření. Stejně jak prvně jmenovaná případová studie WannaCry má stejného nepřímého jmenovatele příčiny takového šíření, což je neaktualizovaný případně nepodporovaný operační systém a jeho užití v zařízení. Rozsah škod způsobený infekcí NotPetya se může řadit minimálně z hlediska finančního mezi jedny z nejnákladnějších a nejničivějších. Incident jako takový se opět váže do roku 2017, konkrétně do 27.6.2017 a do této práce byl spolu s infekcí WannaCry vybrán jako součinitel stejné hrozby jen v jiné časové paralele.

V rámci počátku jeho šíření a charakteristice lze uvést, že stejně jak ransomware WannaCry využíval softwarové chyby EternalBlue (CVE-2017-0144) v protokolu SMBv1, jež byla v časně odhalena Microsoftem a záplatována ve Windows 10. Dále k tomuto ještě ale využíval nástroje psexec a WMI (Windows Management Instrumentation). Zpět zcela prvotně byl objeven analýzou souborů antivirových programů v souborech systému M.E.Doc, kdy software se povětšinou využívá k mzdovému a daňovému účetnictví. (SAI, R. Lakshmi Prasanna a KUMAR, T. Pavan, 2019).

Časovou osu šíření infekce NotPetya z dostupných zdrojů:

- Období do 27.6.2017 – útočící skupinou hackerů je napaden účetní software M.E.Doc, jedná se o napadení aktualizčních serverů, jež následně infikují aktualizaci, jež se zasílá ukrajinským firmám
- 27.6.2017 ráno – dopoledne – infekce NotPetya se začne šířit, využívá k tomu aktualizční systém software M.E.Doc. Primárně jsou tímto softwarem zasaženy Ukrajinské banky, letiště a další kritická infrastruktura
- 27.6.2017 – je zaznamenáno šíření mimo počítačovou síť na Ukrajině. V danou chvíli jsou napadeny systémy společností Maersk (dopravní společnost), Merck (farmacie), Mondelaz (poživatiny)
- 27.6.2017 – infekce již zachycena mimo Evropu, dále se masově šíří do Asie, Severní Ameriky
- 28.7.2017 – jako následek destruktivních snad infekce NotPetya jsou nouzově odpojeny servery jednotlivých společností

Během necelých 48 hodin napáchala infekce NotPetya škody v odhadované výši až 10 mld. USA. Průběh infekce od rána 27.6.2017 až po odpoledne 28.7.2017 byl rychlý a zničující. (tripwire.com, 2017).

Dle správy NÚKIB za rok 2017 byla Česká republika touto infekcí zasažena pouze okrajově, kdy z daných závěrů je patrné, že prvotním a hlavním cílem byla ukrajinská infrastruktura, kdy dále bylo posléze zjištěno ohrožení letišť, metra i provozu jaderné elektrárny.

Ze zveřejněných závěrů odpovědných orgánů vyplívá, že přesto že se infekce NotPetya prvotně zdála jako ransomware, jež má za úkol uživatele napadených zařízení vydírat, při bližší studii bylo zničeno, že jeho úkolem bylo zřejmě masivní likvidace a znehodnocení obrovského množství dat, pozastavení důležitých systémů kritické infrastruktury s cílem zasáhnout především tyto struktury na Ukrajině. To že se infekce následně rozšířila, až do zařízení po celém světě a přinesla dalekosáhlé následky, lze možná chápat jako druhotný jev a jakýsi dominový efekt dané události.

4.3 Vyhodnocení studií

Historické paralely vnímané s ukončením podpory populárního operačního systému Windows 10 se dle provedených analýz nejvíce podobají s obdobím ukončením podpory operačního systému Windows 7 před zhruba 8 lety. Z daného je jasné vidět, že hackerské skupiny, jež mají tyto i jiné infekce na svědomí cílí přímo na dané situace. Přejímové období, kdy je ještě dostatek zařízení bezpečnostně zranitelný takovým způsobem, aby mohli sloužit jako tak zvané „zadní vrátka“ do uzavřeného systému. Ohrožení touto hrozbou nejsou samozřejmě jen jednotlivci a malé firmy, ale především velké organizace, nadnárodní celky a hlavně prvky kritické infrastruktury, jež zde patří:

- Bankovní domy
- Pojišťovací společnosti
- Zdravotnictví
- Veřejné služby
- Energetika
- Veřejný a státní sektor

Obě případové studie jsou si podobné v naprostém začátku, v obou byla využita kritická chyba EternalBlue (CVE-2017-0144), jež následně Microsoft včas záplatoval. V obou případech se jedná o naprosto ukázkovou situaci, co může způsobit nedostatečná aktualizace operačních systémů.

V hodnocení těchto případů můžeme jít ještě dále. Ač se tyto kybernetické útoky neomezuji pouze na daná období, kdy končí jinak populární a masově šířený operační systém, kdy v tomto případě je situace zřejmě u konce podpory Windows 10, tak je nutno uvést že koncentrace těchto situací může být i přesto v těchto obdobích daleko větší. Z toho daného se dá predikovat, že se v obdobné situaci budeme opět nacházet a je jen otázkou času, kdy při vhodném načasování dojde k opětovnému masivnímu útoku.

5 ANALÝZA SOUČASNÉHO STAVU A MOŽNOST ŘEŠENÍ

Bez toho, aby se mohlo rozhodnout přijatí vhodných opatření, musí se napřed analyzovat současný stav a jaké jsou možnosti v této situaci. Konec podpory Windows 10 tedy jednoznačně představuje hrozbu a bezpečnostní riziko. Rozšiřitelnost operačního systému Windows je masová a zařízení, jež může být negativně ovlivněno jsou vyšší čísla milionů.

Tato část, je tedy z daného důvodu rozdělena ve své podstatě na dvě půlky. V první si části jsou analyzovány dostupné možnosti, a to buďto nabízené společností Microsoft případně možnosti dostupné z jiných zdrojů. V druhé části si vyhodnotíme odpovědi na zaslaný analytický dotazník, jež byl konzultován s odbornou částí společnosti Eset, jež je přední slovenský výrobce a distributor masově rozšířeného antivirového programu. V rámci první části byl taktéž pro zprehlednění využity tabulky pro zdůraznění kladů a záporu, jež je jakýmsi kritickým zhodnocení daných řešení, v ostatních případech již hodnotíme řešení v textu, jelikož se nemusí jednat o řešení, jež budou často využitelná, nicméně zmínit je v této práci bylo bezpochyby důležité.

5.1 Možnosti řešení situace s ukončením podpory Windows 10

Některá z možností, jak už bylo uvedeno výše nabízí společnost Microsoft, některé řešení jsou řešením společností třetích stran a některé lze vyvodit z logicky věci. Všechny dané možnosti jsme si tedy analyticky zhodnotili a u každé je dále uveden kladná i záporná část takového řešení.

5.1.1 Migrace na novější verzi operačního systému Windows 11

Naprosto logický krok, jež je v poslední době masivně podporován společností Microsoft. Dalo by se říci, že z dostupných zdrojů, potažmo veřejných prohlášení klíčových činitelů vyplývá, že je to taktéž jediné vhodné řešení. Windows 11 není již nový operační systém a má svoji historii, byl uveden v říjnu 2021. Dle cenové náročnosti se u tohoto OS opakuje situace s Windows 7/8 kdy, pakliže na zařízení je nainstalovaná distribuce Windows 10, lze zdarma upgradovat na Windows 11. Nutno podotknout, pakliže Vám to operační systém Windows díky kontrole kompatibility hardware dovolí, s tím souvisí problém s vyšší HW náročností a jistá specifika, jež jsme si uvedli v teoretické části této práce.

KLADY	ZÁPORY
• Pro konzervativní uživatele se jedná o dobře známé prostředí • Výhledově vyřešen problém s podporou OS, očekávána delší podpora bezpečnostních záplat • Z hlediska bezpečnosti zavádí nové standardy	• HW náročnost, jež je citelně vyšší než u Windows 10 související i ekonomicky vyšší náročnost • Progresivnější sběr dat o uživatelích (ještě více než ve Win10) • Integrace cílených reklam a důraz na jejich prosazování do budoucna

tabulka 1. zhodnocení migrace na Windows 11 (zdroj: vlastní)

5.1.2 Využití programu ESU

Jedná se o další možnost, jež samu nabízí společnost Microsoft. Celý název zní tedy : Extended Security Updates. Microsoft má tuto strategii ozkoušenou již z let minulých, kdy obdobnou variantu využíval řádově již u Windows 7. V dané době nicméně toto využíval pouze pro firemní zákazníky, aby jim nabídnul delší část na adaptaci. V současné době je tento program nabízen i jednotlivcům.

Samotná Microsoft v současné chvíli udává ukončení podpory s využitím programu ESU až 10.10.2028. (Microsoft.com, 2025) Tato služba je nicméně zpoplatněna cenovou politikou, kdy povětšinou je nutný roční poplatek. Tento je výhodný i pro například firemní zákazníky, jež si takto můžou rozvrhnout, datum migrace či jiné vhodné řešení.

KLADY	ZÁPORY
• Možnost oddálení konečného řešení a prodloužení životnosti a nastavení stávajícího • Řešení zaměřeno především na větší firmy, potažmo subjekty kritické infrastruktury (z důvodu složitější migrace dána větší časová flexibilita)	• Pouze bezpečnostní aktualizace, kritické a důležité (samotný systém se již dále nevyvíjí) • Cenová politika aktualizací je agresivní (za každý následující rok vyšší částka) • Není to konečné, pouze dočasné řešení

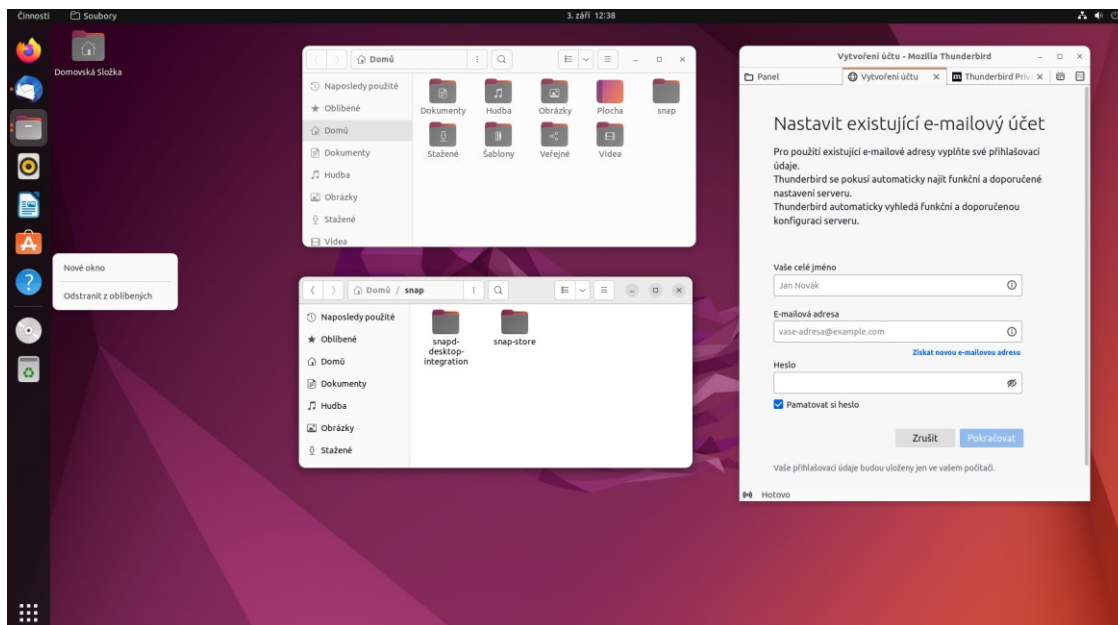
tabulka 2. Využití programu ESU (zdroj: vlastní)

5.1.3 Využití alternativního operačního systému

Možnost zde ještě neprobíraná, nicméně se může jednat o zajímavou alternativu, pro specifický druh zařízení. Alternativou oproti OS Windows může být MacOS, ale v daleko lepším a použitelnějším případě některá z dlouhé škály distribucí založena na Linuxovém jádru. V rámci zabezpečení jednotlivců jen na okraj lze uvažovat tedy i MacOS, jejich funkcionality nicméně se omezujíc pouze na jedince a pro firemní zákazníky, servery a velké společnosti nenabízí dostatečné řešení, z tohoto důvodu dané zmíníme pouze okrajově.

Samotné distribuce Linux je nepřehledné množství na, než by rozhodně nestačila pouhá jedna kapitola. Žebříček distribucí by byl subjektivní nicméně, lze vnímat že populární distribuce Linuxu jsou například:

- Red Hat Enterprise Linux
- Debian
- Ubuntu (grafické rozhraní a jisté prvky ovládání uživatelsky obdobné jak u MS WIN)



obr. 4 Uživatelské rozhraní Ubuntu (PCTUNING,2025)

Tyto systémy jsou hojně distribuovány i do serverových řešení (compare.cz,2024). Nicméně tak jednoduché by to plošným přechodem z Windows na Linux nebylo. Systém jako takový je odlišný především programy, kdy povětšinou programy mnohdy

klíčové běžící na OS Windows neběží v prostředí Linuxu a problematik jako takových je více.

KLADY	ZÁPORY
• Vhodné pro serverové prostředí (pakliže již tedy v daném prostředí server nefunguje) • Nízké náklady na softwarovou licenci • Pro některé vyčlenění se z jisté monopolizace Microsoftu	• Omezený počet odborníků na tuto problematiku plynou z menšího rozšíření systémů Linux • Následně i vyšší náklady na školení personálu • Ve velké míře nekompatibilita softwarových programů z Linuxovými distribucemi (omezení možnosti), toto neplatí, pakliže je používány aplikace z web prohlížeče

tabulka 3. Alternativní OS (zdroj: vlastní)

Na první pohled je přesun na Linuxové distribuce elegantní, nicméně musí být dostatečně připraven a je vhodný pouze pro jistá prostředí, společnosti či prostředí. Na druhou stranu je nutno akcentovat, že v současné době je spousta aplikací a programů schopna fungovat v rozhraní webového prohlížeče, z daného důvodu jsou problémy s nekompatibilitou tímto částečně vyřešeny.

5.1.4 Cloudové řešení Azure

Jak už z názvu napovídá jedná se o řešení v rámci cloud computingu. Toto řešení nabízí opět společnost Microsoft jako další alternativu k užívání osobních počítačů. Je to moderní způsob přístupu uživatelů k softwaru, kdy již daný nevlastníme, nicméně si jej kupujeme prostřednictvím cloudu a výpočetního výkonu společnosti, jež produkt nabízejí. Výhodou pro korporátní zákazníky je bezesporu známe prostředí, jelikož je zde využíván balíček Microsoft Office. Nicméně cloud jako takový má samozřejmě i svou nevýhodu, jež včetně nevlastnění daného softwaru je opět podřízen se cenové politice společnosti Microsoft a jejich ročním poplatkům. Jedná se ve své podstatě o kompletní změnu IT strategie, z hlediska bezpečnosti data a jiné zabezpečuje třetí strana, v tomto případě společnost Microsoft. Z daného nicméně vyplývá, že toto řešení není vhodné plošně pro

všechny možné zařízení. V rámci operace s vysoce citlivými údaji je na zváženu jestli tyto nechat v cloudu kontrolovaném třetí stranou. Vývoj v tomto odvětví je nicméně dynamický a do budoucna, při vhodném nastavení to může být velice využívaná alternativa.

5.1.5 Virtualizace systému Windows 10

Virtualizace Windows je proces, kdy ve své podstatě operační systém běží ve virtuálním prostředí VMware či Hyper-V. Z toho důvodu je nutný i větší výpočetní výkon k udržení takového prostředí. Řešení může být vhodné pro případ nutnosti kompatibility používaného softwaru například s Windows 10, nicméně řešení jako takové není z bezpečnostního hlediska dostatečné, jelikož cílem napadení může být právě virtualizační VMware či Hyper-V. Pro specifické situace a zařízení je to nicméně další možnost jak se vypořádat s ukončením podpory Windows 10.

5.1.6 Off-line režim Windows

Již to zde bylo jednou zmíněno. Když se chceme chránit proti kybernetickým hrozbám, řešení je být odpojen od sítě internet. Nicméně v danou chvíli ale hromada činností, kvůli kterému zařízení máme ztrácí smysl. Použití daného je opět pro specifické případy, ve své podstatě se může jednat o zařízení vevnitř složitých struktur, jež je důležitý pro chod prvku kritické infrastruktury (zařízení ovládající vodovodní přírůdky, kdy není nutné propojení s jiným). Zařízení v off-line režimu by taktéž mělo mít pro jeho dostatečnou bezpečnost odpojení od jiného datového režimu, myšleno tím přenosná média jako USB, CD/DVD, FLASH.

5.1.7 Instalace MS Windows 11 na nepodporované systémy

Z hlediska bezpečnosti, jak už název nepovídá nepůjde o úplně ideální variantu. Jak bylo výše napsáno v teoretické části, Windows 11 má jisté minimální nároky, tyto jsou odvislé i od toho že nový systém přichází s novými formami zvyšování kyberbezpečnosti a aby tyto aspekty mohl do systému aplikovat, musí mít potřebnou hardwarovou výbavu. Z pohledu zařízení se po většinou může jedna o dvě nejčastější situace:

- V zařízení se nachází nepodporovaný procesor, tedy nižší verze než procesor Intel 8. generace, případně AMD procesor starší generace než RYZEN 2000+
- Absence modulu TPM 2.0

Funkčnosti Windows 11 na těchto systémech lze docílit více způsoby, ale hlavní užívané jsou především úpravy registrů Windows, kdy dále pro obejít mechanismů instalace se využívá například nástroj RUFUS, jež dokáže vytvořit takovýto instalační FLASHDISK.

Hrozby pro takto nainstalovaný systém jsou zřejmé. Můžeme začít tím, že Microsoft tyto mechanismy může během nových aktualizací znepřístupnit svými kontrolními systémy, dále samozřejmě jelikož by byli například využívány starší verze procesorů, tyto nemusí mít podporované instrukce, kdy dále i během běhu Windows může docházet k nestabilitě a zvýšenému počtu pádů programů, tedy mohou nastávat problémy s výkonem související od toho, jak moc bude zařízení odlišné od minimálních specifik.

Samotný Microsoft toto sice nepodporuje nicméně na podzim roku 2024 vydal návod, jak tuto možnost oficiálně zprovoznit, kdy cesta zde vede přes upgrade z Windows 10, kdy je dále nabízena možnost, pakliže systém nevyhovuje downgradovat zpět na Windows 10 z Windows 11 (MICROSOFT, 2023).

5.1.8 Setrvání na současné verzi Windows 10 i po ukončení podpory bez aktualizací

Tato možnost je zde zařazena pro účely vyjmenování opravnu všech možností, jež může uživatel využít. Některé jsou možná správné, některé jsou efektivnější, může to záviset případ od případu, nicméně tato varianta je samozřejmě z hlediska bezpečnosti a vyznění celé práce nejméně doporučována a ve své podstatě, by bylo dobré se ji vyhnout. Systém je samozřejmě v daný moment daleko více zranitelnější, jak bude postupovat čas, tak následně se bude dále prohlubovat počet programů, utilit, ovladačů, jež daný systém nebudou podporovat a prostě je na Windows 10 nelze spustit. Pakliže se stane, že toto řešení ba nevědomky dopustí místo jednotlivců organizace menšího či většího rázu na svých zařízeních, tak kromě daleko vyšší míry kyberbezpečností hrozby se taktéž vystavují možnému nedodržení nového legislativního zákona aplikující směrnici NIS 2 a z toho vyplívajících sankcí. Problémů je spousta a jejich popisu se taktéž zabývá významná část této práce.

5.2 Strukturovaný rozhovor – antivirové společnosti

Výše jsme si představovali praktické možnosti řešení ukončení podpory Windows 10 s jednoduše jsme si zhodnotili jejich přínosy ale i negativní stránky věci. Z důvodu komplexnosti této problematiky byl dále vytvořen zámysl kontaktovat nezávislé odborníky v úrovni odborné polemiky, jež by přinesla i jiný náhled do optiky této problematiky.

Dotazy jako takové byli formulovány s ohledem na problematickým přesahem do předmětu Ochrany Obyvatelstva. Jednalo se o tyto dotazy :

1. **Jaká konkrétní bezpečnostní rizika očekáváte po ukončení oficiální podpory systému Windows 10 v roce 2025, zejména v prostředí běžných uživatelů a firem, potažmo státních institucí?**
2. **Je podle Vašeho názoru udržitelný dlouhodobý provoz Windows 10 bez oficiálních bezpečnostních aktualizací při použití moderních antivirových nástrojů a síťové ochrany?**
3. **Jaké řešení byste doporučili organizacím, které z důvodu staršího hardwaru nemohou bez problémů přejít na Windows 11? (např. LTSC verze, Linux, virtualizace...)**
4. **Jaké hrozby představuje setrvání na neaktuálním OS z pohledu české kritické infrastruktury (např. zdravotnictví, doprava, energetika)? Jsou tyto systémy dle Vašeho odhadu dostatečně připraveny?**
5. **Plánujete jako antivirová společnost nabídnout specifická řešení nebo produkty pro uživatele, kteří zůstávají na Windows 10 po roce 2025?**

S touto verzí dotazníku byli kontaktováni odborní pracovníci firmy ESET vydávající stejnojmenný široce užívaný antivirus, jež nabídli odpovědi, z nichž si můžeme opět vytvořit analytické závěry. Pro úplnost je dále třeba uvést, že byli taktéž kontaktováni společnosti Avast, Trustport a Aricoma, kdy zde nepřišla odpověď na možnost strukturovaného rozhovoru.

1. V tomto ohledu se naskytla shodná odpověď s tím, že skutečný dopad konkrétních skutků může být subjektivní nicméně shoda panovala nad tím, že hrozba pro uživatele je značná, především s rizikem na šíření ransomware a obdobných škodlivých infekcí. Jak už bylo v práci jednou zmíněno, s největší pravděpodobností budou nové útoky cílit na již ošetření slabiny a cílit právě na ty uživatele, jež bezpečnostní aktualizace nemají ve svém zařízení. Antivir jako takový může v dané chvíli užitečný při vyhledávání škodlivého softwaru, ale ne při kompletní ochraně systému
2. Praktická použitelnost antivirů jako takových je značně omezena, pakliže dojde k ukončení oficiální podpory dané distribuce Windows, uživatelé mnohdy používají

i starší distribuce, ale obvykle jejich propojení do sítě Internet je pouze omezené, potažmo přecházejí na off-line mód, jež jak jsme uváděli je jednou z možností řešení.

3. Odpověď se sama nabízí v podobě Microsoft Azure, z daných alternativ v případě staršího hardware je toto schůdné řešení. Varianty virtualizace dle uvádění naopak nejsou málo náročné na hardware ba přímo naopak a jejich zachování je vhodně z důvodu daného software řešení, dále Linux je specifický systém, v odpovědi je nabádáno na aspekt finančního ohodnocení administrátorů Linux serverů, jež může být vyšší než administrátorů řešící Windows problematiku.
4. K hodnocení subjektů kritické infrastruktury a jejich řešení chybí především výstupním data, kdy toto nelze předvídat. Hrozby jako takové jsou jednoznačně značné.
5. Společnost ESET dále uvádí z pohledu obou odpovědí schopnost produktů ESET pokračovat v podpoře až do konce roku 2025, omezeně taktéž i pro zákazníky využívající program ESU. Důležité nicméně bylo uvedeno, že pakliže není OS dostatečně záplatovaný, antivir sám osobně ho neochrání a bylo naznačeno, že v dané situaci je nutné dodržet pravidla vícevrstvé bezpečnosti.

5.3 Strukturovaný rozhovor – subjekty kritické infrastruktury

Subjekty kritické infrastruktury je samozřejmě mnoho. Z pohledu této práce bylo zamýšleno se pokusit soustředit na vybrané subjekty ve Zlínském kraji a pokusit se formou strukturovaného rozhovoru zjistit současný stav k prověřované kybernetické události, jež je ukončení podpory Windows 10. Jednalo se o tyto dotazy:

- 1. Používáte (vaše instituce) v současnosti Windows 10?**
- 2. Víte, že podpora Windows 10 skončí v říjnu 2025?**
- 3. Plánujete přechod na Windows 11?**
- 4. Pokud NE, proč? (možno zaškrtnout více možností)**
- 5. Jaké hrozby vnímáte při používání nepodporovaného Windows 10?**
- 6. Jaké řešení uvažujete?**
- 7. Odhadujete, že přechod bude pro vaši organizaci finančně náročný?**
- 8. Máte již plán, jak migraci řešit?**

Zámyslem dotazů bylo vyhodnocení jasný a stručných odpovědí na jasně dané otázky, jež tyto odpovědi by nebyli časově náročné.

Osloveny byli subjekty Krajské nemocnice Tomáše Bati, Krajská úřad Zlínského kraje Nemocnice v Uherské hradišti, Vodovody a kanalizace Zlín, Teplárny Zlín, kdy na výše uvedené odpověděli pouze dva prvně jmenované subjekty. Odpovědi dále jsou řazeny chronologicky za sebou:

1. Ano v obou případech
2. Ano v obou případech
3. Ano v obou případech
4. Z výše uvedeného nevyplněno
5. Zde byli označeny shodně možnost Kybernetické útoky a dále Ztráta podpory ze strany výrobců zařízení
6. Zde je shodně upgrade hardwaru a přechod na Windows 11
7. Dle Krajského úřadu není očekávána vysoká finanční náročnost, kdy je uvedeno že zde vše probíhá již z předstihem, dle KNTB je uvedeno, že finanční náročnost bude značná z důvodu hardwarového zastarání původních zařízení
8. V obou institucích již proces migrace dobíhá

V obou případech lze vysledovat, že bylo využito možnost migrace na Windows 11 spolu s případným upgrade hardwaru. Dále lze zhodnotit, že o dané problematice je na této úrovni, již dobře známo, problematika jako taková je řešena. Hlavní hrozby jsou spatřovány v Kybernetický útocích.

6 MODELOVÁ SITUACE – KALKULACE

V této kapitole bude popsána modelová situace řešení migrace z operačního systému Windows. Nelze se zabývat konkrétní firmou, jelikož konkrétní firmy, subjekty státní správy či samosprávy budou mít v řešení různé nuance, vybereme takový zámysl, jež by procentuálně upravený mohl být akceptovatelný i pro konkrétní subjekty a sloužit jako jakýsi vzor.

Z daného výzkumu, je pro dodržení optimální úrovně bezpečnosti s ohledem na technickou náročnost vhodné především dvě varianty. Těmi jsou migrace na novou verzi operačního systému Windows 11 a jako druhý případ by byl migrace na platformu Windows AZURE. Jistěže z pohledu současnosti se jeví jako relativně nejjednodušší varianta využití programu ESU, nicméně tu momentálně vynecháme, jelikož dané řešení hledáme s výhledem na 3 roky tak aby po těchto mohlo být pokračováno dále.

Zadání situace je prosté. Existuje firma, případně státní instituce jež můžeme anonymně nazývat SUBJEKT A. Tato má ve své užívání 100 zařízení formátu PC. Pakliže se zamyslíme nad počtem užitých zařízení, může se jednat jak o středně velkou firmu, či instituci veřejné správy velikosti například krajského úřadu, krajské nemocnice aj. Tedy se v našem případě jedná o subjekty, jež jsou pro případný kybernetický útok relativně lákavým objektem. Dále si uvedeme, že budeme hledat porovnání pro horizont tedy 3 let, kdy vzato v potaz, je 50 % PC hardwarově nekompatibilní s Windows 11 a je tedy nutný zásadní upgrade obohacený o nové technologie.

6.1 Kalkulace při řešení migrace na Windows 11

Při zámyslu dané situace byl záměrně aplikován postup, kdy 50 % zařízení nesplňuje HW požadavky Windows 11. Tyto zařízení jsou povětšinou stáří 8 a více let a tedy neobsahují kýžené moduly T.P.M. 2.0 stejně jak nepodporované procesory. Při běžném užívání a obměně IT zařízení se může jednat o zcela běžný stav v námi uváděných středních podnicích případně subjektech státní správy a samosprávy. Spolu s danou architekturou v tento moment, je nutné hardwarově nakonfigurovat funkční části PC a jejich cenu. V daný chvíli nebudeme brát v potaz periferie, jež není nutně třeba provést upgradem, ale budeme se pouze zajímat o samotné komponenty. Z daného problému je tedy nutné upgradovat 50 zařízení. Na výpočet kalkulace použijeme běžnou kalkulačku internetového obchodu ALZA.CZ, tak abychom minimálně splnili HW nároky Windows 11.

	1x Procesor Intel Core i3-14100	3 103 Kč Rezervováno pro vás
	1x Operační paměť Patriot Viper Steel 16GB KIT DDR4 3200Mhz CL16	719 Kč Rezervováno pro vás
	1x SSD disk Patriot P210 256GB	439 Kč Rezervováno pro vás
	1x Počítačová skříň Cooler Master MasterBox MB600L V2 Tempered Glass (650W Bronze PSU)	1 599 Kč Rezervováno pro vás
	1x Operační systém Microsoft Windows 11 Home CZ (OEM)	3 115 Kč Rezervováno pro vás
	1x Základní deska MSI PRO H610M-G DDR4	1 699 Kč Rezervováno pro vás
	1x Doprava - AlzaBox	69 Kč Rezervováno pro vás
Celkem k úhradě (včetně DPH)		10 744,00 Kč
K úhradě kartou na místě (nebo zaplatte online předem).		

obr. 5 kalkulace HW upgrade na Windows 11 (zdroj: Alza)

Cena kompletního hardware tedy činí 7629,- Kč pro lepší výpočet a drobné nuance na trhu můžeme brát v potaz, že cena za samotný hardware by se měla pohybovat minimálně okolo 7.500,- Kč + cena Windows 11 HOME (OEM) 3115,-. Tímto lze dojít k částce za upgrade zařízení na celkovou sumu 10.744, -.

Při 50 zařízení to následně výpočtem lze upravit 10.500, - x 50 zařízení = **537.200 Kč**.

V rámci kalkulace byl využit platný ceník e-shopu Alza.cz k 1.5.2025.

6.2 Kalkulace při řešení migrace na Windows AZURE

Opět bude proveden zámysl nad firmou či společností s názvem SUBJEKT A, jež tato má 100 zařízení a řeší případný přechod spojený s ukončením podpory Windows 10. Rozhodnutí v jejich případě padlo na využití Windows AZURE.

Výpočet v tento moment bude rámcově lehčí, nicméně problematika jako takové je dost odlišná. Celkově nastavení Windows Azure klienta a vůbec vybrání si z druhu služby je věc, jež podstatě může ovlivnit užitelnost a cenovou hladinu. Pakliže bereme v potaz zadání, kdy není třeba, aby byli zařízení vybaveny neprůměrným výkonem a postačili si za základní verzi Windows 365, můžeme se dle platných věstníků dostat k ceně asi 41 USD, kdy v současném kurzu se může jednat o 900 Kč / za měsíční pronájem cloudového zařízení.

Při výpočtu $900 * 12 * 100 = 1\,080\,000$ Kč

Při připočtení daného 3letého cyklu se dostaneme na celkovou částku $1\,080\,000 * 3 + 200\,000 = 3\,240\,000$.

6.3 Vyhodnocení modelových situací a jejich možná řešení

Z daných modelových situací je jasně patrné, že jakákoliv řešení pro subjekty menšího až středního charakteru, lze vnímat jejich finanční náročnost v řádech minimálně nižších milionů. Kalkulace Windows AZURE by navíc již při řádově větších řešení o 500–1000 zařízení mohla být velmi zajímavou alternativou, jež do budoucna může Microsoft dále upravovat dle své promyšlené cenové marketingové taktiky. Samotný proces migrace na Windows 11, lze i díky provedení této kalkulace a strukturovaných rozhovorů s odborníky z kritické infrastruktury, hodnotit jako finančně celkem náročný, kdy na něj musí být vyšetřeny nezanedbatelné prostředky.

V potaz v daný moment nebylo bráno počet a plat IT administrátorů, jelikož těchto může být blíže neurčený počet, jelikož je to až příliš závislé na specifikách provozu a firemní IT kultuře, používání doprovodného software atd.

V prvním případě je kalkulace zcela modelová, jelikož závisí na tom, kolik PC v dané firmě je zastaralých a na nepodporovaném hardware. Taktéž při tomto zámyslu můžeme kriticky zhodnotit, že řešení využití v rámci Migrace na Windows 11 a hardwarovému upgradu je myšleno, aby splňovala minimální parametry nicméně situace i celý výpočet bude pozměněn, pakliže bude nutno využívat hardware o vyšším až vysokém výpočetním výkonu.

V daný moment vzhledem například k velikosti větší firmy, již i z pohledu cenové kalkulace může být daleko příznivější řešení migrace přes systém Windows Azure.

ZÁVĚR

Investice do aktualizovaného a podporovaného operačního systému je jak investice do svého zdraví u člověka. Ač nepřináší okamžité prvky, jež bychom mohli pozorovat, tak v dlouhodobém hledisku zajišťuje potřebnou míru bezpečí v tak nebezpečném prostředí jako může být kyberprostor. Pro subjekty kritické infrastruktury a jiné bylo v posledních letech v návaznosti na mnohé bezpečnostní incidenty let minulých, spojených s paralelně podobnou situací, vytvořeno již spousty opatření a vymahatelností i v rámci evropského práva, kdy nejpatrnější a nejdůležitější se zdá být implementace normy NIS 2 a nový český zákon o kyberbezpečnosti, jež bychom se v brzké době měli dočkat. I přesto dle studií obdobných situací lze očekávat, že tvůrci škodlivého softwaru se v přelomový moment, jímž migrace ze současného populárního operačního systému je, pokusí toto využít a kybernetických incidentů bude přibývat.

V poslední části bakalářské práce bylo dále uvedeno, že jak ve světě reálném, tak i ve světě virtuálním není bezpečnost zdarma a nese s sebou jisté finanční investice. Setrvání jako takové na stále pozici, a tedy využívání nadále neaktualizovaného operačního systému není řešením, již pro samotné jedince a malé firmy. S důležitostí a velikostí dané organizace naopak roste palčivost tohoto problému. Řešení jako takových je v nabídce celá řada, ovšem ne všechna jsou vhodná pro každého. Dle studií a analýz bylo zjištěno, že zřejmě nejpravděpodobnější přístup k migraci z Windows 10 bude přechod na Windows 11. Spolu s ním bude společností Microsoft zdůrazňována možnost přechodu na Windows Azure. Z hospodářského hlediska je to pro firmu velikosti Microsoftu velmi lukrativní segment, jež sebou nese nemalé zisky.

SEZNAM POUŽITÉ LITERATURY

- AKBANOV, M., VASSILAKIS, V. G. a LOGOTHETIS, M. D., 2019. WannaCry Ransomware: Analysis of Infection, Persistence, Recovery Prevention and Propagation Mechanisms [online]. [cit. 2025-04-25]. Dostupné z: <https://doi.org/10.26636/jtit.2019.130218>
- AVAST Software s.r.o., 2023. WannaCry: Co je ransomware WannaCry a jak funguje? [online]. [cit. 2025-04-25]. Dostupné z: <https://www.avast.com/cs-cz/c-wannacry>
- CHIP. 500 nejhodnotnějších značek světa: Apple je jednoznačně na prvním místě [online]. Chip.cz, [cit. 2025-04-22]. Dostupné z: <https://www.chip.cz/500-nejhodnotnejsich-znacek-sveta-apple-je-jednoznacne-na-prvnim-miste>
- CISA. Federal Information Security Modernization Act (FISMA) [online]. Cybersecurity and Infrastructure Security Agency, [cit. 2025-04-23]. Dostupné z: <https://www.cisa.gov/topics/cyber-threats-and-advisories/federal-information-security-modernization-act>
- COMPARA.CZ. Jaké systémy Linux instalujeme na servery? [online]. 2023-04-25 [cit. 2025-04-27]. Dostupné z: <https://www.compara.cz/jake-systemy-linux-instalujeme-na-servery>
- COXE, C. Everyday Cybersecurity: A practical approach to understanding cybersecurity, security awareness, and protecting your personal information and identity. [Místo vydání]: [Nakladatel], 2019.
- DELL. Časté dotazy k čipu TPM (Trusted Platform Module) ohledně systému Windows 11 [online]. Dell.com, [cit. 2025-04-22]. Dostupné z: <https://www.dell.com/support/kbdoc/cs-cz/000190999>
- DELOITTE. NIS2: Nová směrnice EU a nový zákon o kybernetické bezpečnosti [online]. [cit. 2025-05-01]. Dostupné z: <https://www.deloitte.com/cz-sk/cs/services/consulting/services/nis2-directive-and-the-new-cybersecurity-act.html>
- ESET. Rootkit. ESET Slovník pojmů [online]. [cit. 2025-04-22]. Dostupné z: <https://help.eset.com/glossary/cs-CZ/rootkits.html>
- GHAFUR, S., KRISTENSEN, S., HONEYFORD, K., MARTIN, G., DARZI, A. a Aylin, P., 2019. A retrospective impact analysis of the WannaCry cyberattack on the NHS. NPJ Digital Medicine, 2, 98. DOI: 10.1038/s41746-019-0161-6.

CHAČATUR, Kryštof. Historie Microsoftu [online]. Sutori, [cit. 2025-04-22]. Dostupné z: <https://www.sutori.com/story/historie-microsoftu--w8ZZPJkKACkXoQBtanZzteVM>

KLATOVSKÝ, Karel. Windows 11: Průvodce uživatele. Praha: Grada, 2022. ISBN 978-80-271-3617-9.

KOLOUCH, Jan. Cybersecurity. Praha: CZ.NIC, 2019. Edice CZ.NIC; svazek 23. ISBN 978-80-88168-33-0.

KONEČNÝ, Martin a Petr SEDLÁK. Kybernetická (ne)bezpečnost: problematika bezpečnosti v kyberprostoru. Brno: CERM, 2021. ISBN 978-80-7204-758-6.

LEGISLATIVA.CZ. Kybernetická bezpečnost – prevence před kyberútoky [online]. Legislativní portál, [cit. 2025-04-22]. Dostupné z: <https://legislativa.cz/zdroje/kyberneticka-bezpecnost/prevence-pred-kyberutoky>

MICROSOFT. History of Microsoft - 1985 [online]. Microsoft Learn, [cit. 2025-04-29]. Dostupné z: <https://learn.microsoft.com/en-us/shows/history/history-of-microsoft-1985>

MICROSOFT. Konec podpory systému Windows [online]. Microsoft.com, [cit. 2025-04-22]. Dostupné z: <https://www.microsoft.com/cs-cz/windows/end-of-support?r=1>

MICROSOFT. Požadavky systému Windows 11 [online]. Microsoft.com, [cit. 2025-04-22]. Dostupné z: <https://www.microsoft.com/cs-cz/windows/windows-11-specifications?r=1>

MICROSOFT. Povolení čipu TPM 2.0 na počítači [online]. Microsoft.com, [cit. 2025-04-22]. Dostupné z: <https://support.microsoft.com/cs-cz/windows/povolen%C3%AD-%C4%8Dipu-tpm-2-0-na-po%C4%8D%C3%ADta%C4%8Di-1fd5a332-360d-4f46-a1e7-ae6b0c90645c1>

MICROSOFT, 2017. Microsoft Security Bulletin MS17-010 - Critical [online]. [cit. 2025-04-25]. Dostupné z: <https://learn.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010>

MICROSOFT, 2023. Windows 11 na zařízeních, která nesplňují minimální požadavky na systém [online]. Microsoft. [cit. 2025-05-01]. Dostupné z: <https://support.microsoft.com/cs-cz/windows/windows-11-na-zaříceních-ktará-nesplňují-minimální-požadavky-na-systém-0b2dc4a2-5933-4ad4-9c09-ef0a331518f1>

Microsoft Corporation. Extended Security Updates [online]. Dostupné z: <https://learn.microsoft.com/cs-cz/lifecycle/faq/extended-security-updates> [cit. 2025-04-27].

NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. Průvodce novým zákonem o kybernetické bezpečnosti [online]. [cit. 2025-05-01]. Dostupné z: <https://portal.nukib.gov.cz/pruvodce-novym-zakonom-o-kyberneticke-bezpecnosti>

NUKIB. Průvodce novým zákonem o kybernetické bezpečnosti [online]. Brno: Národní úřad pro kybernetickou a informační bezpečnost, [cit. 2025-05-01]. Dostupné z: <https://portal.nukib.gov.cz/pruvodce-novym-zakonom-o-kyberneticke-bezpecnosti>

PCTUNING. Rychlý průvodce prostředím Ubuntu a možnostmi přizpůsobení [online]. [cit. 2025-05-01]. Dostupné z: <https://pctuning.cz/article/rychly-pruvodce-prostredim-ubuntu-a-moznostmi-prizpusobeni?chapter=2>

PECINOVSKÝ, Josef a PECINOVSKÝ, Rudolf. Windows 10: Průvodce uživatelem. [Místo vydání]: [Nakladatel], [rok neuveden].

SAI, R. Lakshmi Prasanna a KUMAR, T. Pavan. Reverse Engineering the Behaviour of NotPetya Ransomware. International Journal of Recent Technology and Engineering (IJRTE) [online]. 2019, 8(2S8), s. 1045–1049 [cit. 2025-04-25]. ISSN 2277-3878. Dostupné z: <https://www.ijrte.org/wp-content/uploads/papers/v8i2S8/B12090782S819.pdf>

STATCOUNTER. Windows OS version market share worldwide [online]. StatCounter.com, [cit. 2025-04-22]. Dostupné z: <https://gs.statcounter.com/os-version-market-share/windows/desktop/worldwide#monthly-202403-202503>

STATCOUNTER. Windows Version Market Share Worldwide [online]. Dublin: StatCounter, [cit. 2025-05-01]. Dostupné z: <https://gs.statcounter.com/windows-version-market-share/desktop/worldwide/>

SVĚT HARDWARE. Gordon Moore – zakladatel Intelu a tvůrce Moorova zákona zemřel v 94 letech [online]. SvetHardware.cz, [cit. 2025-04-22]. Dostupné z: <https://www.svethardware.cz/gordon-moore-zakladatel-intelu-a-tvurce-moorova-zakona-zemrel-v-94-letech/59226>

ŠULC, Vladimír. Kybernetická bezpečnost. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 978-80-7380-737-5.

TRIPWIRE, 2017. NotPetya: Timeline of a Ransomware. Tripwire [online]. 30. června 2017 [cit. 2025-04-26]. Dostupné z: <https://www.tripwire.com/state-of-security/notpetya-timeline-of-a-ransomware>

VÍTEK, Jan. FBI zatkla člověka, který registrací domény pomohl zastavit WannaCry. Svět hardware [online]. 7. srpna 2017 [cit. 25. dubna 2025]. Dostupné z: <https://www.svethardware.cz/fbi-zatkla-cloveka-ktery-registraci-domeny-pomohl-zastavit-wannacry/44925>

YOSIFOVICH, Pavel, IONESCU, Alex, RUSSINOVICH, Mark E. a SOLOMON, David A. Windows Internals. Part 1. 7. vyd. Redmond: Microsoft Press, 2017. ISBN 978-0-7356-9774-4.

ŽIVĚ.CZ. Stručná historie Windows [online]. Živě.cz, [cit. 2025-04-22]. Dostupné z: <https://www.zive.cz/clanky/strucna-historie-windows/sc-3-a-115491/default.aspx>

SEZNAM OBRÁZKŮ

Obrázek 1 statistika zastoupení OS Microsoft Windows	22
Obrázek 2 Harmonogram zavádění zákona	29
Obrázek 3 aktivní okno infekce WannaCry	33
Obrázek 4 Uživatelské rozhraní Ubuntu	40
Obrázek 5 kalkulace HW upgrade na Windows 11	48

SEZNAM TABULEK

Tabulka 1 zhodnocení migrace na Windows 11	39
Tabulka 2 Využití programu ESU	39
Tabulka 3 Alternativní OS	41

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

FISMA – směrnice ve Spojených státech amerických, zabývá se aplikováním kyberbezpečnosti

IBM – stěžejní firma stojící za vývojem osobních počítačů

MLD – miliarda

MS-DOS – původní operační systém bez grafické nastavby, předchůdce Windows

NIS – směrnice Evropské unie pro zajištění bezpečnosti v kyberprostoru

NÚKIB – Národní úřad pro kybernetickou a informační bezpečnost

PC – personal computer (česky osobní počítač)

TPM 2.0 – bezpečnostní modul

UEFI – rozhraní důležité při zavádění operačního systému

USD – americký dolar

SEZNAM PŘÍLOH

PŘÍLOHA P I: MAIL S OSLOVENÍM ANTIVIROVÝCH SPOLEČNOSTÍ

Dobrý den,

*rád bych se představil, jmenuji se Lukáš Kozák a jsem studentem kombinovaného studia univerzity Tomáše Bati, fakulty Logistiky a krizového řízení. V profesním životě jsem již pátým rokem policistou a abych se dále profesně i osobně rozvíjel vybral jsem si právě tento obor. Momentálně studuji 3. ročník a dopisuji svou **bakalářskou práci** na téma **Ukončení podpory Microsoft Windows 10: hrozby, udržitelnost a možná řešení**. Vaši instituci jsem se rozhodl kontaktovat s krátkým dotazníkem, jehož částečné závěry bych mohl aplikovat v praktické části své bakalářské práce. Za jakoukoliv pomoc a i částečně zodpovězené dotazy bych byl velmi vděčen a velmi by mi pomohli.*

Dotazy jsou to tyto :

1.Jaká konkrétní bezpečnostní rizika očekáváte po ukončení oficiální podpory systému Windows 10 v roce 2025, zejména v prostředí běžných uživatelů a firem, potažmo státních institucí?

2.Je podle Vašeho názoru udržitelný dlouhodobý provoz Windows 10 bez oficiálních bezpečnostních aktualizací při použití moderních antivirových nástrojů a síťové ochrany?

3.Jaké řešení byste doporučili organizacím, které z důvodu staršího hardwaru nemohou bez problémů přejít na Windows 11? (např. LTSC verze, Linux, virtualizace...)

4.Jaké hrozby představuje setrvání na neaktuálním OS z pohledu české kritické infrastruktury (např. zdravotnictví, doprava, energetika)? Jsou tyto systémy dle Vašeho odhadu dostatečně připraveny?

5.Plánujete jako antivirová společnost nabídnout specifická řešení nebo produkty pro uživatele, kteří zůstávají na Windows 10 po roce 2025?

Jak jsem již sdělil, za jakoukoliv zpětnou vazbu od Vaší firmy budu velmi vděčen.

s pozdravem

a přání hezkého dne

student FLKR UTB a uživatel

Lukáš Kozák

PŘÍLOHA P II: MAIL VYBRANÝM SUBJEKTŮM KRITICKÉ INFRASTRUKTURY

Vážené dámy, vážení pánové,

jmenuji se Lukáš Kozák dovoluji si Vás oslovit jako student Fakulty logistiky a krizového řízení Univerzity Tomáše Bati ve Zlíně (kombinovaného studia) v rámci zpracování bakalářské práce na téma:

„Ukončení podpory Microsoft Windows 10: hrozby, udržitelnost a možná řešení“.

V praktické části práce se zaměřuji na identifikaci potenciálních bezpečnostních rizik, možností přechodu na jiná řešení a dopadů na kritickou informační infrastrukturu v České republice.

Byl bych velmi vděčný, pokud byste mohli věnovat chvíli vyplnění několika krátkých dotazů (dotazník je tvořen na vyplnění během 5 minut), které mají sloužit jako podklad pro analytickou část mé bakalářské práce.

Dotazník – Windows 10 a bezpečnost kritické infrastruktury:

1. Používáte (vaše instituce) v současnosti Windows 10?

- Ano
- Ne

2. Víte, že podpora Windows 10 skončí v říjnu 2025?

- Ano
- Ne

3. Plánujete přechod na Windows 11?

- Ano
- Ne
- Nevíme zatím

4. Pokud NE, proč? (možno zaškrtnout více možností)

- Nevyhovující hardware
- Vysoké náklady

- Nevidíme důvod měnit
- Zvažujeme alternativní systém (Linux, MacOS apod.)

5. Jaké hrozby vnímáte při používání nepodporovaného Windows 10?

(vyberte maximálně 2 možnosti)

- Kybernetické útoky
- Problémy s kompatibilitou softwaru
- Ztráta podpory ze strany výrobců zařízení
- Nepovažujeme to za problém

6. Jaké řešení uvažujete?

- Upgrade hardware + Windows 11
- Přechod na cloudové služby (Windows 365)
- Pokračování s Windows 10 + rozšířená bezpečnostní podpora
- Jiná varianta (uveďte jaká): _____

7. Odhadujete, že přechod bude pro vaši organizaci finančně náročný?

- Ano, výrazně
- Částečně
- Ne

8. Máte již plán, jak migraci řešit?

- Ano
- Ne

Děkuji Vám mockrát za spolupráci

s podravem

Lukáš Kozák