Historie IT

a blízkých témat

Obsah

Předmluva

Kniha vznikla jako můj o projekt během studia na střední škole. V rámci jednoho z předmětů jsem měl během celého roku pracovat na projektu, v který věřím a jenž by měl praktické využití. Nenapadlo mě žádné technické řešení, které by nějakým způsobem neexistovalo a neměl jsem zájem pracovat na sobeckém projektu, jako jsou osobní webové stránky. Zároveň jsem chtěl, aby v případě, že se na projekt někdo podívá, dostala daná osoba z knihy přidanou hodnotu. Měla by se o něco obohatit a něco se dozvědět i po letech, kdy tato kniha nebude nová.

Od mala jsem rád psal, četl a také jsem rád studoval historii. Ať už skrze videohry, či knihy. A tak jsem se rozhodl spojit to, co aktuálně studuji s tím, co miluji od raného věku. Vznikl tak nápad na tvorbu knihy, která by popisovala co nejvíce historii počítačů a souvisejícími odvětvími. Je těžko popsatelné, o čem všem jsem chtěl, aby kniha byla. Zkrátka jsem chtěl popsat co největší kus historie počítačů. Nevěděl jsem však co přesně bude ještě obsahem knihy.
V rozhodnutí o obsahu mi mimo jiné pomohli předměty, které jsem se během studia učil. Zároveň témata, kterým jsem se věnoval a považoval jsem je

za důležitá. Za celý rok jsem však nebyl schopen sepsat to, co se stalo za jedno století, a tak nechávám místo pro další doplňky, které bych mohl uskutečnit v budoucnosti. Či by je mohl doplnit nějaký jiný zájemce.

Rád bych v závěru předmluvy poděkoval svým rodičům a příbuzným za podporu, kterou mi během celého studia i během psaní poskytovali. Poděkovat chci i kamarádům a spolužákům, kterým se nápad zamlouval a navedli mě tak k jeho realizování.

Speciální poděkování patří paní učitelce Mgr. Tereze Krausové, která mi po celou dobu psaní dělala konzultantku a podporovala mě při psaní, byť jsem jí do jisté míry zklamal jako učitelku češtiny a mnohokrát chyboval po gramatické stránce.

Michal Koudela

Kryptologie

„Lidská vynalézavost nevymyslí šifru, kterou by lidská vynalézavost nedokázala rozluštit.“

- **Edgar Allan Poe, Graham's Magazine 1841**

Kryptologie, jak název pro znalce řečtiny napovídá, je nauka o šifrování. „Krypto“ může svádět k interpretaci jakožto nauce o kryptoměnách. Ty naopak prvky z kryptologie využívají, ale sami nejsou jejím hlavním cílem.

Proč potřebujeme šifrovat? Cílem šifrování je utajit zprávu a její obsah před nechtěnou stranou. Záleží nám na našem soukromí a nechceme, aby naši zprávu mohl číst kdokoliv. Také nám záleží na tom, aby tuto zprávu nikdo nezměnil a aby byla vůbec doručena. Těmto třem podmínkám se říká CIA – Confidentiality, Integrity, Availability (neplést s americkou tajnou službou) neboli důvěrnost, neporušenost a dostupnost. Kryptologie se zabývá především prvními

dvěma. Dostupnost je otázka přenosových médií, například Internetu či Flash Disku.

Proč ale toto téma probírat v knize o IT? Důvod je jednoduchý. Hlavní vývoj počítačů souvisí se snahou vytvářet a prolomit nové bezpečné šifry a jiné šifry prolomit. Už během druhé světové války Němci používali šifrovací stroj *enigma* a spojenci v Anglii v čele s *Alanem Turingem* vymysleli stroj, který tuto šifru dokáže prolomit. Od té doby se vymýšlely šifry, které měly být proti těmto strojí neprolomitelné a naopak stroje, které šifry prolamovaly. Tato šifrovací kampaň tak silně podpořila vývoj počítačů.

My se tedy podíváme na výběr z historie šifrování a také na to, jak fungují, potažmo kam směřuje blízká budoucnost šifrování.

Kryptografie

Kryptografie je podobor kryptologie se zaměřením na šifrování, šifrový design a jejich tvorbu. Jakákoliv šifra potřebuje šifrovací **klíč**. Tím může být další krátká zpráva, číselná konstrukce či náhodný sled znaků a symbolů.

Rozdělit kryptografii bychom mohli na ***symetrickou*** a ***asymetrickou*****.** Symetrická kryptografie a její šifry používají stejný klíč k šifrování i dešifrování.

Asymetrická kryptografie je naopak složitější a pomocí matematických problémů a funkcí, šifruje jedním klíčem a dešifrují jiným. Lze vyjádřit vztah mezi těmito dvěma klíči. Jednou z bezpečnostních podmínek je však neodvoditelnost **soukromého** klíče z **veřejného**.

Kryptoanalýza

Kryptoanalýza je disciplína zabývající se **luštěním** šifer bez znalosti klíče a zprávy. Součástí je analýza, prolomení a hledání chyb v šifrách. Takovémuto člověku se říká kryptoanalytik.

Steganografie

Steganografie je zvláštní část kryptologie, která se zabývá ukrýváním zpráv do jiných zpráv. Historicky by se mohlo jednat o schovávání zpráv v obrazech. Či například napsáním zprávy na kus papíru podle šablony a následně dopsání slov tak, aby zpráva byla zjistitelná pouze pomocí šablony, která se k papíru přiloží. I dnes se používá steganografie hojně v počítačích, kde je možné schovat soubor do jiného souboru. Například schováním textového souboru do souboru obrázku. Pomocí jiné či té samé aplikace se pak textový soubor z obrázku extrahuje (Steghide).

Historické šifry

Zprvu se podíváme na historické šifry. Jsou dobře známé, a proto by se neměly používat. Maximálně pro „utajovanou“ komunikaci mezi spolužáky během hodiny. V tomto případě nás však zajímá spíše vývoj šifrování a jak jsme se časem dostali k šifrovým systémům, které máme dnes.

Vznik písma – cca 3000 let př.n.l.

Než vůbec můžeme začít mluvit o tom, jaké byly první šifry musíme si říct, co se šifrovalo. Lidé nemluví plynule v šifrách, i když se tak občas může jevit. Šifry vznikly hlavně jako způsob utajení písma.

Jedny z prvních důkazů o existenci písma lze nalézt na území dnešního Iráku. Tehdejší Mezopotámie, kde žila civilizace Sumerů, kteří byli jedni z prvních uživatelů **klínové písmo.** V tom je zapsaný i známý Epos o Gilgamešovi.

V podobnou dobu se v Egyptě začali vyvíjet znaky, které dnes známe jako hieroglyfy. Existuje i případy používaní zvláštních upravených hieroglyfů, pravděpodobně se tak mohlo jednat o jednu z prvních šifer vůbec.

Atbaš - *6. století př.n.l.*

Atbaš byla šifra vymyšlena Hebrejci a spočívala v záměně (**substituci**) písmene vždy s písmenem stejně daleko v abecedě, ale z druhého konce. Její výskyt můžeme najít i v bibli.

V naší české abecedě by se pak ABC zapsalo jako ŽZY.

Skytalé - *5. století př.n.l.*

Mezi Sparťany v antickém Řecku se začal používat první nástroj pro utajení zpráv. Jednalo se o *skytale*. Válcovitou tyč, na níž byl obvázán pruh kůže se zprávou. Když se tento provázek rozmotal bylo pořadí písmen pomícháno a nikdo bez stejného válce nedokázal zprávu rozluštit.

Jednalo se o jednu z prvních **transpozičních** šifer. Transpozicí nazýváme tedy promíchání pozic znaků mezi sebou.

Potetovaný otrok - *5. století př.n.l.*

Herodotos ve svých dějinách popsal incident, jak Řek jménem Histeautus nechal oholit svému otroku hlavu a vytetoval mu na ni skrytou zprávu s informacemi o povstání proti Peršanům. Když otrokovi narostly vlasy zpátky poslal jej zprávu doručit.

Jednalo se o jednu z prvních využití steganografie, jehož hlavním cílem bylo zprávu skrýt nikoliv zašifrovat. Samozřejmou nevýhodou je doba čekání, než vlasy dorostou.

Nirabhasa a Arthasatra – 3. století př.n.l.

V Indii vzniká počátek znakové řeči. Tehdejší Nirabhasa slouží pro komunikaci mezi obchodníky a kupci. Využívá klouby a konečky prstů.

Arthashatra je kniha z Indie, která poprvé zmiňuje prolamování kódů a využití šifer pro politické účely.

Polybiův čtverec – 2. století př.n.l.

Polybius navrhuje způsob vizuální signální komunikace na delší vzdálenosti. Každé písmeno abecedy je zapsáno do políčka ve více řádkovém a sloupcovém čtverci. Každá řada a sloupec jsou očíslovány. Zvednutá pochodeň pravou a levou rukou určují pak číslo sloupce a řádku.

Jedná se o jeden z prvních případů převodu písmen na čísla. To v dnešních počítačích samozřejmostí a jednalo se tak o pravděpodobnou inspiraci.

Caesarova šifra a římská vojenská kryptografie – 64 př.n.l. až 16 n.l.

Římané v armádě prokazatelně používali šifry pro komunikaci mezi legiemi. Jeden ze způsobů bylo psaní latinských textů v řecké abecedě. Gaius Julius Caesar potom používal šifru, kde každé písmeno nahradil písmenem o tři místa před ním. Augustus jeho adoptivní synovec používal stejný systém, ale místo o tři pozice šlo o jednu. S výjimkou X, které se nahrazovalo AA.

Caesarova šifra se dá vyjádřit i jako:

$$(A + 3) \bmod 26 = D$$

Kde A je písmeno, které má být zašifrováno, C je výsledné písmeno a 26 je počet písmen v abecedě. V tomto případě se má A hodnotu 1 a D hodnotu 4.

Mod je operace modulo, která ukazuje zbytek po dělení.

Př. 5 mod 2 = 1

Blízký východ – 8.až 9. století

Na Blízkém východě v okolí Bagdádu se shromáždilo spoustu informací o matematice, medicíně, astrologii, ale také o šifrách. Při pátrání po původních slovech proroka Mohameda v islámské víře, využívali arabští učenci metodu, kterou dnes nazýváme jako **frekvenční analýza**. Ta funguje na principu toho, že vezme jakýkoliv text z jednoho jazyka a získáme statistiku nejpoužívanějších písmenek. Potom vezmeme počet symbolů v šifře a porovnáme jej s počty výskytu jednotlivých písmen v naší abecedě. Tento způsob kryptoanalýzy funguje převážně na klasické substituční šifry, kde jsou znaky či písmenka zaměněna mezi sebou. Také se těmto šifrám říká **monoalfabetické**. Několik z významných mužů této doby je zde zapsáno společně s jejich prací.

Abu `Abd al-Rahman sepisuje knihu Kitáb al-Mu'amma. Kniha byla napsána pro byzantského císaře a pojednává o řešení šifer. Jedná se o jednu z prvních kryptoanalytických knih. **Alkindus** vytváří a sepisuje vlastní způsob prolomování šifer pomocí frekvenční analýzy. **Abu bakr Ahmad ben Alí** zapisuje několik klasických šifer používaných pro „magii“ do své knihy.

Ballymote – Konec 14. století

Kniha sepisuje dohromady vyluštěné dříve používané šifry. Šifrovací „Runy“ se používali převážně v Anglii a severských zemích. Nejznámější variantou je „Isruna“ původní verze, od které se všechny další odvozovali.

Homofonní šifra – 1401

Vzniká první homofonní šifra vytvořena Simeone de Cremo z Mantovy. Oproti klasické substituci se zde jeden znak nahrazuje větším počtem jiných znaků. To komplikuje frekvenční útoky na šifru. Do budoucna bude vznikat mnoho druhů homofonních šifer.

Jan Hus – 1415

Při svém uvěznění v Kostnici posílá Hus dopisy, kde jsou samohlásky nahrazeny písmenem, které leží po dané souhlásce. A je zapisováno jako B. E jako F.

Vigenère- 1586

Vigenère sepisuje svou knihu „Traicté des chiffres“. V té zdokonaluje některé systémy a popisuje některé šifry. Jeho největším úspěchem je zdokonalením Cardonova šifrovacího autoklíče. První verzi navrhl Girolamo Cardano, nicméně bez Vigenèra by se nepoužíval. Také je známá jeho propagace **polyalfabetických** šifer místo doteď používaných

monoalfabetických. Jeho vylepšení jsou ale degradovány, a nakonec je po něm pojmenovaná šifra o dosti primitivnější než jeho navrhovaná vylepšení.

Takzvaná „Vigenèrova šifra“ funguje následovně. Vezme-li písmeno A a klíč k němu bude písmeno B. Pak nám vznikne písmeno B. Začínáme totiž počítat od nuly.

Zprávu: **PESALEKJEHODNY**
Klíč: **HODNY**
Výsledek: **WSVNJLYMRFVRQL**

Poté co písmeno L zašifrujeme písmenem Y.
Pokračujeme s klíčem znovu pomocí písmena H.

Anglie - 1587

Ve Skotsku schvaluje Marie Stuartová atentát na královnu Alžbětu I. Dává souhlas s atentátem na královnu v jednom ze svých zašifrovaných dopisů. U soudu pak byla usvědčena a odousouzena k trestu smrti. Dopisy se totiž podařilo rozluštit díky podrazu jednoho z Mariin blízkých, který byl na své místo poslán jako špeh královnou Alžbětou.

De Augmentis Scientarum – 1623

Sir Francis Bacon vytváří šifru, kterou bychom dnes mohli považovat za binární kódování. Pomocí změny fontů ji pak může zakódovat do jakékoliv zprávy. Z části se tak jednalo o kódování, ale díky svému utajování v knihách se z části jedná i o steganografii. Která vždy využívala 5 písmen zapsaných po sobě v textu jiným fontem. Zpravidla se jednalo o písmeno „a“ a písmeno „b“.

Pořadí písmen a odchylky v podobě písmene b pak vytvářelo šifru takto:

aaaaa = a aaaab = b

aaaba = c

Prezidentův nápad – 1790 až 1800

Americký prezident Thomas Jefferson vymyslel během života šifrovací přístroj, který předčil svou dobu. Za jeho života nebyl však nikdy vyroben a jeho návrh se našel až v roce 1922 v Knihovně Kongresu USA. Po úpravách byl používán u amerického námořnictva až do 70‘ let minulého století. Jefferson pak dostal také přezdívku „Otec americké kryptologie“.

Máchův deník - 1835

Mácha vedle svých básní napsal v roce 1835 deník. Jisté pasáže deníku byly ovšem zašifrované Máchovou vlastní šifrou. Jakubu Arbesovi se je ovšem o přibližně 40 let později podaří rozluštit. Zjišťuje však, že jejich obsah je spíše především sexuální, a tak kvůli českému národnímu obrození a nově vznikajícímu kultu okolo Máchy se rozhodne dešifrované části nepublikovat. Hrozí riziko, že by tím mohl český národ pohoršit. Máchův deník vychází poprvé až v 70‘ letech 20. století.

Telegraf - 1840

Samuel F. B. Morse patentoval a vynalezl telegraf. Zařízení, které umožňovalo relativně rychlou komunikaci na velké vzdálenosti pomocí signálu. Ten byl vypnutý či zapnutý. Tento popis dvou stavů se nám může jednat dnes povědomí.

Krátké zapnutí představovalo tečku a ty dlouhé zapnutí čárku. Z toho se pak vytvořila abeceda, která byla **zakódována** (neplést se zašifrováním). Účelem kódování totiž není zprávu skrýt. Ale upravit ji do vhodného formátu. Více si k telegrafu řekneme v kapitole Počítačové sítě.

Kasisky– 1863

Pruský důstojník publikoval knihu o šifrách, ve které popisuje metodu luštění Vigenérovy šifry, kde se klíč po čase opakuje. Ukazuje tím na slabinu a dokazuje, že by klíč měl být stejně dlouhý jako zpráva samotná.

One-Time-Pad – 1882

Během roku 1882 vyslovil Frank Miller domněnku, že chceme-li zaručit skutečnou bezpečnost šifry, tak klíč k šifře musí být stejně dlouhý nebo delší, než je samotná zpráva. Klíč musí být předán ještě před samotnou zprávou a ta bude zašifrována pomocí modulární operace. Například pomocí bitové operace XOR. Tento princip je aplikovatelný a platí do dnes. Nevýhodou je, že klíč má stejnou či větší délku než samotná zpráva a museli bychom zaručit i jeho bezpečné přenesení v případě zachycení klíče stačí šifru snadno dešifrovat. V roce 1942 pak Claude Shannon potvrdil matematickou bezpečnost OTP, ovšem s podmínkou, že vygenerovaný klíč je opravdu náhodný a nikdy se znovu nepoužije.

To však nezabránilo, aby se v budoucnu v nepoužil.

Pro ukázku zde uvádím tabulku, jaké jsou hodnoty pro logickou operaci XOR:

A	B	Y
0	0	0
0	1	1
1	0	1
1	1	0

Voynichův rukopis - 1912

Wilfrid M. Voynich našel knihu v jednom malém italském městečku. Dodnes se jedná o jednu z nejtajemnějších knih. Její obsah je sbírkou šifrovaných textů s obrázky o květinách, astronomii a zvířatech. O knize stále moc nevíme. Pouze její předešlé autory mezi, které patří například i Rudolf II.

Válečná a poválečná období

Během válek se stále vyskytovaly klasické šifry. Kvůli nutnosti bylo, ale do jejich luštění vynaloženo mnohem více snahy. Také díky objevům posledních let se některé šifry staly zcela nevhodné a primitivní na vyřešení. Bylo teda potřeba změny.

Šifry se během válek a chvilku po ní odvíjely hlavně podle šifrovacích strojů. Ať už se posílaly přes telegram, šifrovaly se přes německou enigmu či japonskou PURPLE. Mechanické šifrátory se pak nějaký čas ještě používali, než se přešlo na počítače,

které z části vznikly i pro počítání náročnějších příkladů. To zas umožnily rozvoj matiky se šifrováním.

Zimmermannův telegram - 1917

Během první světové války Německo vědělo, že situace se vyvíjí v prohru. A tak jako jeden z posledních snah o změnu průběhu války, nechalo poslat přes svého špióna v americkém kongresu do Mexika telegram. Tento telegram byl však zachycen a rychle rozluštěn anglickou vládou. Obsahem byla nabídka pro mexickou vládu, že v případě útoku na USA jim bude dána podpora Německa a americká území budou po právu rozdělena.

Když se Spojené státy o tomto dozvěděly, okamžitě Německu vyhlásily válku. Do západní fronty se tak zapojily americké jednotky nativních indiánů, kteří přes rádia posílala ve svém rodném jazyku tajné zprávy s informacemi.

Proč, ale Anglie zprávu zachytila? Jako jeden z prvních válečných aktů, ne-li první váleční akt Anglie vůči Německu bylo přetrhnutí podvodní telegrafického kabelu mezi Německem a Amerikou. Amerika byla totiž počátkem války nestranná, vzhledem k tomu že velká část jejích kolonizátorů byla právě z Německa. A tak obchodovala s oběma stranami. Německo bylo

pak nuceno komunikovat s Amerikou přes telegrafovou linku vedoucí přes Anglii. Snaha o šifrování komunikace tak byla veliká, ale ve výsledku málo účinná.

Enigma – 1933-1945

Enigma zajisté je jedna z nejznámější šifer či možná tou nejznámější šifrou všech dob. Jednalo se o šifrovací stroj založený na mechanický rotorech patentovaný Hugo Kochem. Ten však komerčně neuspěl a patent prodal Arthurovi Scherbiovi, který stroj vylepšil a prodával pod názvem Enigma. Stroj také prezentoval během francouzského poštovního veletrhu a Německo si jej na tolik oblíbilo, že jej používalo po celou dobu 2. světové války.

První člověk, který enigmu prolomil byl Polák Marijan Rejewski. To se mu podařilo pouze na prvotních verzích enigmy a během průběhu celé druhé světové války tyto varianty luštil a předával britům. V mezičase se zřídila speciální skupina v Bletchley Parku. V čele s Alanem Turingem, Dillym Knoxem a Gordonem Welchmanem se jim podařilo přijít na způsob, jak vyluštit nové verze Enigmi pomocí **Brute-Force** útoku. Tedy vyzkoušení všech možných kombinací. To samozřejmě přispělo k pádu nacistického Německa.

Stroj, který pomohl prolomit Enigmu se jmenuje Bombe. První verzí ještě před válkou vyvinul Rejewski. Po invazi Němců do Polska ji byl však nucen zničit, aby zamezil Němcům v zjištění, jak funguje. Druhá varianta vznikla v Anglii pod Turingem a dokázala najít klíč, byť byla zpráva zašifrována na dvakrát. Výtvor v roce 1942 pak sdíleli i s Američany. Ty díky zreprodukování a rozšifrování zpráv z německých ponorek zachránily tisíce životů. Bohužel byla tato americká varianta zničena kvůli psychickému zhroucení jejího stvořitele.

Turing je také známý pro svou teoretickou práci o výpočetní síle a teorie strojů. Mezi jedny z nejznámějších věcí je jeho test. Tedy Turingův test, který má za cíl odlišit člověka od stroje. Tento test sloužil i jako inspirace pro sci-fi či filmovou sérii Blade Runner.

Štolba – 1935

Štolba byla jedna z prvních, ne-li prvním československým šifrovacím přístrojem. Pravděpodobně byl navržen dle nákresů Hugo Kocha s rozdílem, že oproti Engimě a ostatním šifrovacím strojům založeným na rotorech. Nepoužíval k pohybu rotorů elektriku, ale vtlačený plyn. Na stroji se podílela zbrojovka Brno nejspíše, která vyráběla i šifrovací stroj typu Z. Který je téměř identický štolbě.

Štolba je pojmenována po pplk. Josefu Štolbovi, který byl pověřen ministerstvem obrany k tvorbě šifrovacího stroje.

PURPLE – 1939

PURPLE byl šifrovací stroj používaný Japonci po celou dobu 2. světové války. Byl založen na používání telefonních součástek. Američané tento šifrovací stroj prolomily a princip jeho šifrování utajovali až do 70. let minulého století. Kdy byly zveřejněny.

Po válce se všechny existující stroje zničili.

ENIAC – 1946

Američané vyvinuli první kompletně elektronický programovatelný stroj schopný vypočítat řadu příkladů. Oproti strojům tehdejší doby byl kompletně elektronický a jeho výroba stáal 500 000 $. Obsahoval přes 17 000 elektronek a přibližně 5 milionů ručně pájených spojů.

SIGABA – 1950

Během druhé světové války používali Američané šifrovací stroj označován jako SIGABA či ECM. Jako. Jediný během druhé světové války byl Němci neprolomen. Jeho princip fungování je podobný

enigmě. S tím rozdílem, že při každé nové zprávě se válce posunuli do opravdu náhodné polohy.

M-125 - 1956

Rusové po konci druhé světové války přišli s odpovědí na americké šifrovací stroje v podobě „Fialky“. Ten se stal hlavním šifrovacím strojem pro státy Varšavské smlouvy, včetně Československa.

Stroj byl svým principem podobný enigmě, ale měl 10 rotorů a pro každou zemi varšavské smlouvy byla unikátní varianta s jejich abecedou. To samozřejmě odpovídalo upraveným součástkám. Stroj byl také dodán Kubě jakožto spojenci.

ČS OTP – 1960 až 1990

Během celé studené války Československo používalo systém One-Time-Pad pro komunikaci se svými ambasádami v zahraničí. Poslalo vždy dvě obálky, kartičku červenou a modrou, které obsahovali nutné kódy a čísla. V případě porušení ochrany kartiček by se znehodnotily a nedaly by se použít.

Moderní šifrování

S příchodem počítačů jako nové rychlejší výpočetní síly se musely přizpůsobit i šifry. Po období magnetických pásek přišla doba bitů. Ty nabývají dvě

hodnoty. Pravda a nepravda. Jedna či nula. V 70‘ letech pak začala teorie výpočetní rychlosti a počítače, které počítali rychleji, než lidé se stali hlavním způsobem počtů. Šifrování se přesunulo na digitální scénu a místo mechanických a logických strojů se začali používat počítače.

Mikročip – 1958

Tohoto roku vynalezli fyzici Jack Kilby a Robert Noyce první integrovaný obvod z polovodiče. Oba tak učinili nezávisle na sobě. Tímto bylo možné kondenzátory, tranzistory a odpory spojit do jedné malé křemíkové či germaniové destičky.

To je obrovský skok ve vývoji počítačů.

LUCIFER – 1970

Horst Feistel vymyslel ve firmě IBM šifru Lucife, jako jednu z prvních **blokových** šifer. Ta v budoucnu inspiruje spoustu dalších, které se stanou šiframi Feistelova stylu.

Blokovou šifrou rozumíme takou, která rozdělí zprávu do bytových bloků a ty následně šifruje stejným klíčem. Proudové šifry naopak každý blok šifrují klíčem jiným či jinou částí klíče.

P vs NP – 1971

Teoretický problém, který je stále aktuální, v roce 1971 vyslovil ve své práci „T*he complexity of theorem proving procedures*“ (volně přeloženo jako teorie komplexnosti výpočetní procedury) Stephen Cook.

Tento problém říká, že máme-li problém u kterého počítač může ověřit pravdivost s výsledkem za jistý čas. Měl by být za stejný čas schopen vypočítat reálnou hodnotu daného problému. Obecně je předpokládáno, že rovnost mezi těmito dvěma časy není. A že existují problémy, které je těžší vyřešit než ověřit. Nicméně tento problém nebyl matematicky potvrzen ani vyvrácen.

Aktuálně je vystavěna odměna 1 000 000 $. Na řešení, které bude světovými institucemi uznáno.
V kryptografii by řešení tohoto problému znamenalo, že pro každý bezpečnostní algoritmus existuje algoritmus stejně rychlý a optimální, který by šifru dokázal prolomit.

DES – 1976

Jednou z takových je i Data Encryption System. Který upravuje National State Agency (NSA) a stal se americkým standardem v šifrování. Později se jedná o

jednu z nejrozšířenějších šifer na světě. Problém šifry v budoucnu bude, že používá 56bitový klíč (+ 8 bitů).

V roce 1993 pak vychází najevo že existuje stroj, který dokáže vyzkoušet všechny možné kombinace do 7 hodin.

O dva roky později 1995 pak NSA vlastní stroj, který je tuto šifru schopen vyřešit všechny kombinace do 15 minut.

V roce 1997 je pak přes internet proveden pokus o prolomení 56bitového klíče za využití výpočetní síly několika počítačů z celého svět. Tento pokus je úspěšný a DES není nadále bezpečné.

Diffie-Hellmannova výměna klíčů – 1976

Whitfield Diffie a Martin Hellman poprvé ve svém článku navrhují šifrování a dešifrování odlišným klíčem. Bylo to počátky asymetrické kryptografie, neboť útočník by byť po získání klíče, v tomto případě veřejného, neměl být schopen šifru vyluštit. Matika za tímto problémem je v podobě diskrétního logaritmu. Celý problém se dá shrnout tak, že je těžké získat X z následujícího příkladu, byť známe všechny ostatní proměnné.

$$y = g^x \bmod p$$

Uživatel A a B si náhodně zvolí **p** a **g**. Každý si pak zvolí svůj tajný soukromý exponent **a**, **b.** Uživatel A pak odesílá **y** = g^a mod p. Uživatel B pak odesílá **x** = g^b mod p. Následně uživatel A vypočítá $\mathbf{x^a}$ **mod p** to by mělo být rovno $\mathbf{y^b}$ **mod p**. Tímto způsobem si oba uživatelé můžou vyměnit třeba klíč od šifry přes nebezpečný kanál. I tento bezpečnostní systém má však bezpečnostní vady a je ohrožen útokem MIM (Man In the middle). Kdy útočník stojí mezi oběma stranama.

RSA – 1977

Vzniká první systém na základě asymetrické kryptografie pojmenovaný podle svých autorů Ronald L. **R**ivest, Adi **S**hamir, Leonard M. **A**dleman. Tento algoritmus funguje na problému faktorizace velkých prvočísel. Platí že:

$$n = p * q$$

Pro počítač je součin snadný, ale faktorizování n na p a q je problém. Musí projít všechny možné kombinace, a to je problém. První

V roce 1994 se pak nelezl rozklad 129ciferného čísla. To je pro RSA bezpečnost velký problém a ukázalo to na nutnost prodloužení délek klíčů do budoucna.

Tento problém se opakoval v roce 1999 kde se našel rozklad čísla o délce 155cifer neboli 512 bitů.

Dnes se doporučuje délka klíče alespoň 2048 bitů.

Salt – 1979

Takzvaná sůl se poprvé používala na unixových systémech, kde sloužila jako přídavek k heslům před procesem hešovaní (probereme níže), aby se zamezilo riziku kolize a zvýšila se tak bezpečnost.

Poprvé se tak hesla v souboru /etc/shadow ukládala se solí. Soubor samotný slouží k ukládání hesel a ověřování hesel s jednotlivými uživateli. Tedy náhodně vygenerovaným přídavkem, který zabránil kolizi.

Kvantové počítače – 1981

V tomto roce fyzik Richard Feynman navrhuje tvorbu kvantových počítačů, které by místo klasických bitů používali **qubity**. Neboli elementy, které jsou současně jedna i nula. Proces počítání a operací by se tak neuvěřitelně zvýšil. Bylo odhadnuto, že by taký počítač mohl provést až 2^{1000} operací za vteřinu. Tedy tolik operací že je to více než počet atomů v našem vesmíru. Či větší než částka pokuty uvrhnutá na společnost Google Ruskou vládou tento rok. Nicméně by toto science fiction dále od pravdy. Kvantové počítače

Některé asymetrické šifry založené na problému faktorizace či diskrétním logaritmu, by se tak zcela znehodnotily a byly by v budoucnu nepoužitelnými. Prevencí tohoto potencionálního problému se zabývá post-kvantová kryptografie.

Největším číslem, které se ověřitelně podařilo faktorovat kvantovým počítačem byl číslo 21 v roce 2012 pomocí Shorova algoritmu. Jedná se o dosti nízké číslo. Nicméně se v průběhu let objevily záznamy o dalších faktorizacích již poměrně vyšších čísel. V roce 2016 se podařilo faktorizovat číslo 200 099 pomocí procesoru **D-Wave** 2X. V roce 2019 i číslo 1 099 551 473 989. Nicméně tento případ byl kritizován, neboť využíval klasických počítačů, aby proces zmenšil na příklad, jenž vyžadoval pouze 3 qubity. D-Wave ještě v roce 2024 vydalo dokument tvrdící výsledky o faktorizaci čísla 8 219 999 pomocí nového QPU (Quantum Processing Unit) – kvantové procesní jednotky D-Wave Pegasus.

Nutno dodat, že byť se všechna faktorizovaná čísla zdají veliká, opak je pravdou. Čísla využívána v asymetrické kryptografii jsou mnohem větší a v porovnání s těmito jsou gigantická.

Kvantové kryptografie – 1984

Charles H. Bennett a Gilles Brassard se zasloužily o teoretické využití kvantových počítačů v kryptografii. Následně přišli s algoritmem BB84, prvním bezpečným kvantový protokolem pro distribuci klíčů.

ECC – 1985

Byl představen problém diskrétního logaritmu na eliptické křivce jako alternativní a efektivnější způsob pro asymetrické kryptografii. Z hlediska bezpečnosti je 256bitový klíč u ECC efektivnější než 4096bitový klíč u RSA. Problém je však komplikovanější, a tak se pořádné implementace dočkal až v roce 2005 kdy začal být podporován v softwaru OpenSSL a 2011 kdy přibyla možnost do OpenSSH. Využití našel v kryptoměnách a v zařízeních Apple.

MD2 – 1989

Hešování vzniklo již dříve, ale teprve od roku 1989 začala vznikat série algoritmů MD. Neboli „Message Digest“ s kterými přišel Ronald L. Rivset, jeden z autorů RSA.

Hešování je jednosměrný proces konvertování dat do staticky velikého formátu. Tedy soubor o velikosti 2 GB projedeme algoritmem MD2 a vznikneme nám ideálně unikátní výstup o velikosti 128 bitů. Pokud však dá jiný

soubor stejný výsledek. Dochází ke kolizi což je nežádoucí.

K čemu je to dobré? Ve zkratce tím můžeme ověřit pravost dat mezi dvěma stranami. Vezmeme-li soubor z jedné strany kde je zároveň napsán jeho heš můžeme soubor stáhnout a nechat ho zahešovat ve stejném algoritmu. Budou-li se výsledky shodovat znamená to, že soubor je opravdu soubor z webu a nikoliv jiný, který chtěl například útočník zaměnit. Je to jeden ze způsobů, jak ověřovat integritu v praxi.

Aby hešovací algoritmus fungoval musí nám dát vždy stejný výsledek pro stejný vstup a nesmí se z výsledku získat vstup. Mezi další algoritmy vytvořené Rivsetem patří **MD4** (1995), **MD5** (1996) a **MD6** (2008). MD5 se považuje již prakticky za prolomený a neměl by se používat praktické implementaci.

PGP – 1991

Pretty Good Privacy byl program který používá pro šifrování IDEA, což je alternativní vylepšená verzi DES. A pro přenos klíčů využívá RSA. Jeho tvůrcem je Phil Zimmermann. Ten vyvezl zdrojový kód programu z USA načež bylo na něj podáno trestné stíhání. V roce 1996 pak bylo toto stíhání ukončeno.

SHA – 1993

Secure Hashing Algorithm je hešovací algoritmus, který byl navrhnut NSA a FIPS. První návrh pochází z roku 1993 a dnes je označován jako **SHA-0**. Nikdy však nebyl určen pro veřejné účely a o dva roky později (1995) se z něj vyvinul **SHA-1**, který produkoval 160bitový výstup. Nutnost vylepšení prvotní verze se dokázala v roce 2004, kdy prolomily SHA-0. SHA-1 zůstalo neprolomeno až do roku 2017. Zajímavým faktem zůstává že pro vývoj SHA-1 bylo inspirací MD4.

SHA-2 je rodina hešovacích algoritmů z roku 2003. Patří sem algoritmy s bitovým výstupem o velikostech 224, 256, 384, 512. Tato rodina algoritmů se dodnes používá v protokolech jako jsou TLS, PGP, SSH, IPsec. Dodnes je tato rodina algoritmů stále bezpečná, nicméně je stále pod pokusy najít kolizi.

SHA-3 bylo výběrový proce (podobně jako u AES), který skončil výhrou hešovací algoritmu Keccak. Začalo v roce 2006 a skončilo 2012 vítězstvím algoritmu Keccak, který byl pak standardizován v roce 2015. Je však důležité podotknout, že SHA-3 nemá nahradit SHA-2 a má sloužit jako alternativní hešovací způsob.

HMAC – 1996

HMAC vznikl jako algoritmus, který ověřuje integritu a autenticitu zprávy. Princip fungovaní je taký že ke zprávě připojíme heš s klíčem dva spojeného s hešem zprávy a klíče jedna. Graficky bychom mohli HMAC zobrazit takto:

$$H\,(H\,(Z \,||\, K_1) \,||\, K_2)$$

V tomto případě H značí hešovací funkci, $K_{1,2}$ jsou klíče odvozené z jednoho primárního klíče. || pak znamená že pouze spojujeme prvek nalevo s prvkem napravo. Pro hešování se nejčastěji používá SHA-256. Lze však použít i s jinými heši. V roce 2008 byl HMAC pak standardizován americkým úřadem NIST.

3DES – 1997

Poté co vychází najevo, že je DES nadále nepoužitelné, používá se jako provizorní řešení 3DES. Tedy tento algoritmus funguje na třech klíčích. Zpráva se jedním zašifruje. Odšifruje druhým. A nakonec znovu zašifruje třetím. Protože je DES symetrický šifrovací systém lze jej stejným způsobem dešifrovat. Tím se sice náročnost na luštění zvyšuje. Bylo však otázkou času, než se i tento problém vyřeší. A tak NIST (Americký národní úřad pro standardy a patenty) vyhlašuje soutěž o šifru AES. Nástupce DES.

V roce 1999 se pak uzavírají návrhy na novou AES šifru.

AES – 2000

Vítěz soutěže o novou AES šifru je Rijndael. Navržený dvěma belgickými studenty MIT. Místo 64bitového klíče používá tři varianty. 128, 192 či 256 bitů. Je spočítáno že prolomení takovéhoto klíče při správné implementaci a útokem typu brute-force by trvalo přibližně okolo 20 triliard let pro 128bitový klíč.

Post-kvantová kryptografie – 2024

V letošním roce NIST schválila tři nové standardy v post-kvantové kryptografii, ML-DSA, ML-KEM, SLH-DSA. Jak jsem již dříve nastínil post-kvantová kryptografie má za cíl najít nové šifry či vylepšit ty staré tak, aby nebyly schopné být prolomeny kvantovými počítači. Jedná se o asymetrické šifry a systémy založené na problému faktorizace a diskrétních logaritmu. Tedy šifry jako RSA a sytém Diffie-Hellmann jsou v budoucnu v ohrožení. Jak jsme si však uváděli kvantové počítače nejsou stále aktuálně dostatečně výkonné pro řešení vysokých čísel, byť by k tomu často mohou články o tématu svádět. Pro příklad v roce 2019 společnost Google tvrdila že ve spolupráci s NASA vyvinula kvantový počítač jenž dokáže během 200 vteřin vypočítat příklad, který by nejvýkonnějšímu

počítači (SUMMIT) na světě trval 10 000 let. Společnost IBM tvůrci toho počítače však odpověděli že výpočet takého příklad trval 2.5 dne. Nejedná se tedy o takové zrychlení, jak se může v médiích tvrdit.

Internet a počítačové sítě

„Všichni jsme teď spojeni internetem, jako neurony v obrovském mozku.“

- **Stephen Hawking, Q&A with Stephen Hawking, USA TODAY TECH**

V této kapitole se budeme bavit o vzniku a historii internetu. Povíme si jaké komunikační prostředky internetu předcházeli, jak vznikaly první sítě a jak se rozšířily po celém světě. Koukneme se na vznik webových stránek a na to, jak se využil internet ke zločinu v podobě Dark Webu.

Historie telekomunikace a internetu

Dálková komunikace prošla dlouhým vývojem. První byly poslové, kteří si zapamatovávali dlouhé zprávy svých pánů, aby je pak bezchybně zopakovali.

Používali se také i kouřové signály, ty využívali například Indiánové. S příchodem písma se začali posílat dopisy, které pokud měli pečeť zaručovali i integritu zprávy. Nakonec s vynálezem telegrafu přišla doba elektronické komunikace, načež navázali telefony a dnes internet.

Podstata všech těchto technologií je teda ve snadné a dostupné komunikaci. Spojování lidí napříč vzdálenostem je příležitost, jak rozvíjet všechny odvětví lidské činnosti. I tak bychom tedy mohli pohlížet na internet. Jako na možnost propojení lidí všech lidí napříč světem. Důležité však podotknout, že byť byly tyto technologie vytvořeny s dobrými úmysly, našli se tací, kteří je využívají pro šíření dezinformací a vlastní prospěch. Tohoto faktu bychom si měli být vědomi a brát na něj zřetel vždy kdy čteme články z internetu.

Telegraf

V roce 1837 představil Samuel Morse přístroj, jenž spojuje dvě místa kabelem. Pomocí jeho nástroje pak vysílal elektronický signál. Tento signál je na druhé straně přijat a v závislosti na čase jeho trvání je zapsána čárka nebo tečka, tedy dlouhý nebo krátký signál. Podle univerzální tabulky se pak zapsané signály převedou na písmenka a vytvoří se zpráva.

Tento styl kódování vymyslel sám Morse současně s přístrojem.

V roce 1866 se pak zavedla linka mezi Evropou a Amerikou. O čtyři roky později pak vznikla i linka mezi Amerikou a Austrálií, která mohla být následně informována o všem co se ve světě děje. Ve stejném roce i přímá linka mezi Anglií a Amerikou.

Thomas Edison vylepšil v roce 1876 způsob jakým se signál přes kabel odesílá a umožnil tak pomocí jednoho kabelu posílat až čtyři zprávy v jeden moment.

Nakonec však telegrafová linka upadla oproti technologiím, které ji předčily. Poslední odeslaný telegraf Českou poštou byl v roce 2010. A Austrálie, která na této technologii těžce závisela, oficiálně skončila provoz telegrafu v roce 2013.

Telefon

Alexandr Graham Bell v roce 1876 patentoval přístroj dnes známý jako telefon. O rok později pak založil svou společnost pod jménem Bell Telephone Company. Ta se dnes jmenuje **AT&T** a pokud jste o ní neslyšeli jedná se o jednu z největších telekomunikačních společností na světě, která se zabývá poskytováním internetového připojení, vývojem nových technologií a bezdrátovými technologiemi.

Telefon vznikl jako přístroj pro přenos hlasu přes kabel. Oproti telegrafu tak bylo výhodou přímá a rychlejší komunikace. Okamžitě se stal velice populárním a úspěšným.

V roce 1904 vznikl známý French phone, který se šířil i do domácností. V 1921 se technologie zlepšila a přes dva kabely se dali vést tři komunikace. Během a druhé světové války byla nutnost komunikace za pohybu. Telefony tak začali užívat **elektromagnetické vlny** podobně jako rádia a byly tak schopny komunikovat „bezdrátově". Nakonec se technologie vylepšila i na používaní mikrovlnných vln, které mají vyšší frekvence. V roce 1961 se pak do vesmíru odeslal první mezinárodní komunikační satelit.

Od osmdesátých let zažily obří „bum", kdy se začali šířit v podobě **mobilních telefonů**. V roce 1982 představila společnost Nokia vůbec první mobilní telefon *Mobira Senator*. Nevýhodou byla váha, která byla 10 kilogramů. O rok později přišli s vylepšenou verzí *Motorola Dynatac 8000X,* kde váha činila už „pouhý" jeden kilogram. Doba výdrže tohoto telefonu byla 30 minut a nabíjel se 10 hodin.

V roce 1992 pak Nokia představila revoluci v podobě mobilu *Nokia 1011*. Ten využíval technologii GSM, které si jinak říkalo **2G**. V roce 2000 pak Nokie

představil opět jednu z dnešních legend *Nokia 3310*. Tento telefon si vydobyl pověst nerozbitné cihly, která vydrží téměř všem tíhovým testům. Další revoluce přišla v roce 2007, kdy proslulý Steve Jobs představil **IPhone**. Mobilní telefon s dotykovou obrazovkou s možností stahovat aplikace, hrát hry, surfovat po internetu a nepoužívat tak telefon pouze pro komunikaci. Byť již pár let takováto technologie existovala, příchod IPhonu na trh se považuje za opravdovou revoluci v tomto odvětví mobilním telefonům se tak začne také přezdívat **smartphone**. IPhone má za svůj operační systém IOS, ke kterému o rok později v roce 2008 vznikne open-source konkurence v podobě Androidu. Ten je založený na Linuxu a oproti konkurenci je modulární a upravovatelný.

V roce 2009 se ve Švédsku a Norsku spustily první komerční implementace **4G** též známé jako **LTE**. A v roce 2019 se v Jižní Koreji spustila první komerční **5G** síť. Implementace 5G v České republice, ale i na světě spolu nesla velké problémy, neboť vzniklo spoustu konspiračních teorií o nepříznivém vlivu 5G na lidské tělo. Tyto teorie byli však vyvráceny, u nás ČTU, který se veřejně snažil vysvětlovat vliv frekvencí na lidskou tkáň. Za zmínění stojí i 6G, budoucí technologii

zkoumá u nás laboratoř na Fakultě Elektrotechnické ČVUT.

Internet

Po druhé světové válce spousta amerických organizací experimentovalo s počítači a v případě kdy jich vlastnili více potřebovali vytvořit mezi těmito počítači univerzální komunikační systém. Tak vznikali první malé sítě jednotlivých organizací, které byly izolované a malé. Používali vždy způsob komunikace vytvořený danou organizací, a tak se těžko dalo komunikovat s jinými sítěmi.

„Na počátku byl **APRANET**“. Píše Ed Krol ve svém stopařově průvodci po internetu (RFC 1118) při snaze definovat jeho historii. Amerika byla po druhé světové válce plně ponořena ve studené válce a chystali se scénáře na katastrofické události. Jedním z problémů, která americká vláda měla, byla potřeba **decentralizované** komunikace mezi státními organizacemi. Tento způsob komunikace by musel vydržet jaderný útok. Návrhem byla pověřena společnost RAND Corporation. Ta přišla s jednotnou sítí pojmenovanou podle agentury dohlížející na tuto zakázku ARPANET (společnost se jmenovala ARPA). Cílem projektu bylo pospojovat všechny malé pro stát důležité sítě a vytvořit mezi nimi jednu velkou hlavní síť.

Mezi cílové sítě patřily hlavně univerzity jako je ta v Los Angeles a společnosti jako je NASA. Tato velká síť ze začátku používala jeden ucelený protokol pro komunikaci se jménem **NCP** neboli *Network Control Protocol*.

V roce 1969 pak měla skupina vysokoškoláků (Vinton Cerf, Steven Crocker, Jon Postel) za cíl monitorování a testování na sítí ARPANET. Své poznatky zapsali a vydali je jako „požadavek o komentář“. Request-For-Comment neboli **RFC** poprvé definovalo protokoly jako je IP, TCP, FTP, SMTP. Této sbírce protokolů a jejich vztahů, které se stali globálně uznávanými, dnes říkáme **TCP/IP**.

ARPANET dosáhl patnácti uzlů v roce 1971. Které se o dva roky později rozrostli na 35 s tím že se ve stejném roce připojilo i Norsko a Anglie. Ten samý rok proběhla i první implementace TCP/IP do reálně sítě. A v roce 1977 návrh tohoto modelu završil. V roce 1982 pentagon schválil přechod všech počítačů v síti ARPANETu na používání TCP/IP modelu namísto zastaralého NCP. Tento model s dalšími vylepšeními používá celý internet dodnes. Svou roli sehrál i BSD Unix, který jako operační systém nepřímo podporovaný DARPA (přejmenovaná ARPA) cílil na implementaci nového modelu.

Na síť se pak nabalovali další menší sítě. Celá síť pak dostala příhodně pojmenovaný Internet. Později se ARPANET ještě spojil s NSFNET. Obě tyto páteřní sítě pak časem zanikly. 1986 se pak k velké síti připojují další instituce a od této doby používání internetu roste exponenciální křivkou. Internet už nemá žádného vlastníka. Jedná se o abstraktní spojení všech malých sítí. Platí se například pouze příspěvky firmám, které poskytují připojení pro menší firmy za výdaje s tím spojené. V Americe jsou tyto firmy především AT&T a General Atomics.

V Československé republice se internet stal věcí až po pádu komunismu v roce 1989. Hlavním problémem byla česká infrastruktura, která nebyla na internetu vůbec vybudována. Používali se tak slabší technologie, které umožňovali komunikaci přes telefonní linky. V roce 1990 se několik počítačů připojilo do takzvané EUnet, který propojuje Unixové počítače v Evropě. Koncem tohoto roku pak na ČVUT vznikl první uzel pro komunikaci s EARN. Evropskou sítí spojující akademické a vědecké instituce.

13. Února 1992 se Československá republika oficiálně připojuje k internetu. Ve stejném roce pak vzniká po dohodách CESNET (Czech Educational and Scientific Network). Jeho cílem je rozšíření přístupu k internetu

mezi hlavní vědecké a vysokoškolské instituce v Česku. Rozvod přístupu k internetu po městě měl být pak však koncipován jinými společnostmi.

Od té doby u nás původně telefonní společnosti jako je dnes O2, Vodafone, T-Mobile začali nabízet připojení k internetu. Páteřní linkou českého internetu však zůstává CESNET.

V roce 1997 nastal další velký krok na poli internetového připojení, a to v podobě standardu 802.11 od Americké standartové společnosti IEEE. Definuje využití vysokých frekvencí k přenosu dat a připojení k internetu. Dnes tuto technologii známe jako Wi-Fi. S příchodem dostupných routerů nabízející tuto technologii se tak internet dostal téměř do každé domácnosti.

Na závěr si dovolím vyložit jednu úvahu. Dnes původně decentralizovaný internet již tak docela decentralizovaný docela není. Velké společnosti jako je Google a Amazon díky svým obřím ziskům investovala do velkých datových center, která fungují jako centralizované uzli. Internet tak bude fungovat bez nich. Ale protože většina webových stránek a internetových služeb funguje uvnitř těchto datacenter tak by velká část internetu bez nich nefungovala.

Zamyslete se sami, které webové stránky používáte denně a leží v takových to centrech.

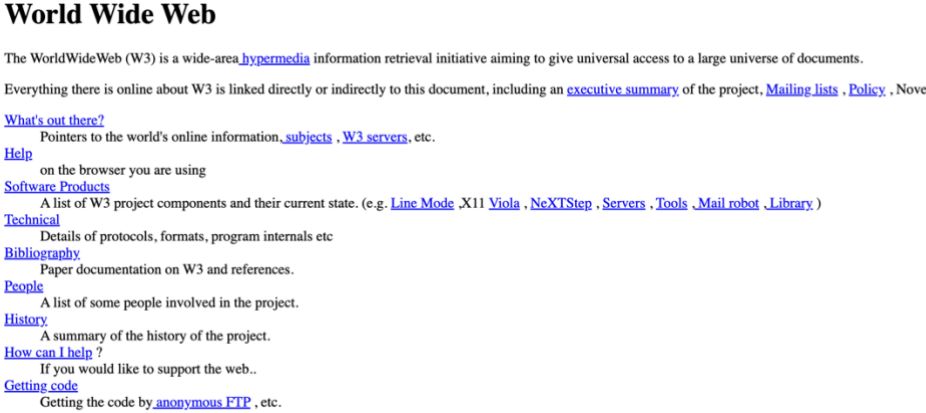
World Wide Web

Když existoval internet. Vznikla i potřeba po rychlém šíření informací z důvěryhodných zdrojů. **WWW** se ale vyvinul v to co si dnes představujeme pod internetem. Stal se sbírkou všech informací, různých nabídek služeb a produktů. Uložištěm našich souborů a zprostředkovatelem sledování videí. Web jako takový je pro všechny, kteří mají přístup k internetu způsobem, jak s ním interagovat. Ať už čtete článek, posloucháte hudbu, nebo se koukáte na video, využíváte webových stránek. Co víc aplikace, které na mobilu používáte mohou být pouze kopiemi webových stránek přizpůsobený pro snadnější používání. Zkrátka dnes je web denním chlebem. Jak jsme ale k němu přišli?

Web 1.0

S prvním návrhem WWW přišel Tim Berns-Lee, když pracoval pro Švýcarskou firmu CERN v roce 1989. Jednalo se o poměrně abstraktní přenos informací využívající hypertext, který by mohl přenášet hypermédia. O rok později definuje ve své druhé práci tři základní pilíře fungování WWW. Ty jsou **HTML**,

HTTP a **URL**. HTML neboli *HyperText Markup Language* je jazyk, ve kterém jsou webové stránky definované. HTTP je *HyperText Transportation Protocol* a ten říká, jak se bude HTML přenášet mezi dvěma počítači. URL je pak zodpovědný za nalezení konkrétních dokumentů, jedná se o vždy o adresu daného HTML. Adresa se zadá do prohlížeče a vede k webovému serveru. Koncem téhož roku představuje první prohlížeč a editor (Browser) a následně spouští a ukazuje první funkční web. Vypadá takto a popisuje samotný WWW projekt:



World Wide Web

The WorldWideWeb (W3) is a wide-area hypermedia information retrieval initiative aiming to give universal access to a large universe of documents.

Everything there is online about W3 is linked directly or indirectly to this document, including an executive summary of the project, Mailing lists , Policy , Nove

What's out there?
Pointers to the world's online information, subjects , W3 servers, etc.
Help
on the browser you are using
Software Products
A list of W3 project components and their current state. (e.g. Line Mode ,X11 Viola , NeXTStep , Servers , Tools , Mail robot , Library)
Technical
Details of protocols, formats, program internals etc
Bibliography
Paper documentation on W3 and references.
People
A list of some people involved in the project.
History
A summary of the history of the project.
How can I help ?
If you would like to support the web..
Getting code
Getting the code by anonymous FTP , etc.

Zdroj: (https://info.cern.ch/hypertext/WWW/TheProject.html)

V srpnu 1991 pak ohlašuje existenci WWW softwaru na internetu. V prosinci pak vzniká první webová stránka mimo Evropu. Stanfordské centrum lineárního urychlovače jej využívá pro přenos

interních informacích pro zaměstnance v sekci vysoko-energetické fyziky. Počet webových stránek na celém internetu roste. V roce 1993 vzniká webový prohlížeč Mosaic pro windowsový operační systém X. Stejný rok je WWW oficiálně veřejné vlastnictví a CERN se vzdává jakýchkoliv práv. V roce 1994 je na celém světě přes 10 000 webových stránek. Stejný rok ještě Berns-Lee zakládá World Wide Web Consortium (**W3C**), které bude mít WWW na starost a vydá sbírku standardů definující chování světového otevřeného webu. (Viz. www.w3.org/standards)

Nějaké z principů těchto standardů jsou decentralizace, veřejný kód stránky, nulová diskriminace kvality služeb.

V roce 1994 se Håkon Wium Lie a Bert Bos podílejí společně s W3C na tvorbě **CSS**. Cascading Style Sheets je nový jazyk, který slouží jako doplněk HTML. „Suchý“ text a elementy upravuje v barevné a lépe vypadající stránky. Všechny designové úpravy tak jak je známe dnes, jsou dělané přes CSS. První implementace se povedla v roce 1996 pod jménem CSS1. V roce 1998 se přešlo na vylepšenou CSS2. V roce 2011 pak na CSS 2.1 a dnes se používá CSS3, která byla vydávána postupně. Dnes se vyvíjí CSS 4.

Web 2.0

Od předchozí abstraktní verze se liší v zapojení uživatelů do obsahu na stránce. Nejde už jen o pouhou četbu webového dokumentu, ale opravdovou interakci. To bylo docíleno s příchodem **JavaScriptu** (JS). Ten byl navrhnut Breidnem Eichem v roce 1995 a jmenuje se tak protože slovo Java bylo v té době dost populární. Tento jazyk se brzy standardizoval a zpopulárnil. Dnes je ale mezi vývojáři občas kritizován pro některé chyby, ty připustil i autor. Přechází se na **TypeScript** (TS), který vydali inženýři z Microsoftu v roce 2012. Ten se však stejnak překládá do JavaScriptu a tak se vše zdá marné. Zkrátka Javascript je již zakořeněn mezi prohlížeči i uživateli. To z části nepřipouští jakoukoliv změnu.

JavaScript byl a je tak populární, že dal vzniknout takzvaným frameworkům. To jsou v podstatě sbírky předělaného kódu, který vývojářům ulehčuje a zefektivňuje práci. Mezi významné patří React (2013), jQuery (2006), Node.js (2009), Svelte (2016) a Angular (2010). Existuje jich však spousta dalších.

Co dále definuje Web 2.0 je příchod sociálních sítí včele s Facebookem, později Twitterem a Instagramem. Celé nové odvětví sociálních komunikace raději přenechám sociologům. Myslím si

ale, že se všichni shodneme, že příchod sociálních sítí měl obrovský dopad na naši společnost.

Web 3.0

Web se stal centralizovaným. Kvůli velkým společnostem vlastnící data centra jako je Amazon, Google a Microsoft hostující milióny webových stránek, nastalo porušení zásady o decentralizaci webu. Vznikají tak nové projekty, které mají fungovat jako alternativa a návrat k decentralizaci.

Mimo to má však další verze webu zapojit do svého fungování mnohem více umělou inteligenci, internet věcí (IoT) a 3D grafiku. Zkrátka nápadů, co by další verze webu měla dělat je mnoho.

Při definování těchto webových verzí je však brát velké zohlednění na abstraktnost této problematiky. Nikde přesně není definováno jak první, druhá či třetí verze vypadají. Pro nás se tak jedná spíše o přiblížení témat.

Prohlížeče

Pár následujících stránek dedikuju jednotlivým prohlížečům, které nám dávají přístup k World Wide Webu. Je třeba se zamyslet nad realitou, kdy tyto prohlížeče ať chceme nebo ne, mohou sledovat naše soukromí. Doporučují nám reklamy na základě jejich

zákazníků a profitují z nás. Myslete na to až si budete příště vybírat svůj prohlížeč.

Internet Explorer

Internet Explorer je prohlížeč tradičně dodávaný spolu s operačním systémem Windows. Poprvé se tak stalo v roce 1995 kdy Microsoft vydal svůj operační systém Windows 95. Jeho součástí byl i tento prohlížeč, která byl vyvinut na základech zdrojového kódu Mosaicu. Jednalo se o jeden z prvních prohlížečů po Mosaicu. Díky tomu, že Internet Explorer podporoval nové technologie jako bylo v tu dobu CSS a ActiveX stal se velice populárním. Dostával také pravidelně bezpečnostní updaty. Během následujících let byl nejpoužívanějším prohlížečem na světě. V roce 2015 jej nahradil Microsoft Edge, ale to popularitu příliš nevylepšilo. Dnes se vtipkuje především o tom, že Explorer nebo Edge je na počítači pouze od toho, aby se stáhl Google Chrome.

Google

Dva studenti se během roku 1995 rozhodli začít společnost, která se stala jednou z největších společností na světě, oficiálně byla založena, ale až o tři roky později. Larry Page a Sergey Brin tak učinili, jak již bývalo tradicí v garáži s minimálními prostředky.

Vytvořili vyhledávač, který se původně jmenoval Backrub a později byl přejmenován na **Google**. Hlavním cílem mělo být utřídění všech informací na internetu. Tento prohlížeč zaujal jejich akademickou scénu a investory ze Silicon Valley, v česku známého jako křemíkového údolí. V roce 1998 dostali šek na 100 000 dolarů a díky velkému úspěchu se z Googlu stala jedna z největších společností na světě. V následujících letech pohltil a vytvořil spoustu nových firem. V roce 2004 koupil společnost Keyhole, Inc., která se přejmenovala na Google Earth. Ve stejném roce pak vznikl Gmail. V roce 2006 pak koupil Youtube, která přinesla veřejná videa na internet. Dnes je opravdu spoustu produktů, které firma nabízí. Pokud se zajímáte, ale o zajímavé spory doporučuji si pustit seriál „The Billion Dollar Code“, která ukazuje německý projekt TerraVision, který se až moc podobá Google Earth a to vznikl mnohem dříve.

Mozilla (Firefox)

Projekt **Mozilla** byl založen v roce 1995 a stal se komunitní prací o vytvoření veřejného, dostupného a transparentního prohlížeče. Jedná se tak o jeden z open-source prohlížečů tedy takých prohlížečů, který neskrývají svůj zdrojový kód a uživatel si může dohledat přesně co prohlížeč dělá pomocí jeho kódu.

V roce 2002 se publikovala Mozilla 1.0 jedna z prvních hlavních verzí softwaru. Protože ale až 90 % uživatelů používala Internet Explorer nebyla moc populární. Projekt však nezanikl a v roce 2003 vznikla separátní nezisková firma Mozilla Foundation. Ta měla na starost získávání zdrojů pro vývoj prohlížeče. V roce 2004 vyšel Firefox 1.0 a stal se velkým úspěchem s počtem stáhnutí přes 100 milionů za jeden rok. V roce 2013 pak vznikl vlastní operační systém pro mobily (Firefox OS), který měl za cíl přiblížit dostupné a privátní vyhledávání uživatelům na mobilních telefonech. Do dnes zůstává hlavními cíli Mozilly transparentnost a soukromí.

Další prohlížeče

Mezi další významné prohlížeče patří například **Opera**, která je původem Norská, ale nyní je vlastněna většinově čínskými akciovými firmami. Mezi mladou generací se teď stává populární kvůli prohlížeči pro „gamery“.

Dalším zajímavým prohlížečem je **Brave**. Který založil Breiden Eich tvůrce JavaScriptu. Jedná se o prohlížeč založen na Chromiu. Veřejně dostupným kódu od společnosti Google. Hlavním cílem prohlížeče je soukromý a bezpečnost na internetu. Ve výchozím nastavení automaticky odstraňuje reklamy. Brave také

nabízí možnost zapnout
Brave-Ads kdy vrací uživatelům 70 % částky, kterou inzerant zaplatil za reklamu. Tato částka je vyplácena v kryptoměně BAT.

Dark Web

Zvláštní částí internetu jak celku a world wide webu, je Dark web. Často se o něm mluví jako o něčem tajemném a zlém. Není to však pravdou. Dark web se dnes především označuje přístup k webovým stránkám přes TOR síť, **The Onion Routing**. Síť funguje na principu Onion routingu. Připojíte se k serveru, ten je součástí TOR sítě. Server zároveň skrývá veškerou vaši aktivitu na internetu a vy byste tak měli být anonymní. V teorii, pokud byste byli sledováni státním orgánem či velkou korporací, existoval by záznam o vašem připojení do TOR sítě. Nebylo by však zjistitelné, co zpoza tohoto serveru děláte a kam se připojujete. To se liší od klasického prohlížeče, kde v teorii, jsou entity schopné stopovat vaše vyhledávání a vaši aktivitu na internetu. Nikoliv však po připojení k TOR síti. Rozdíl s komerčními

V roce 1995 David Goldschlag, Mike Reed a Paul Syverson zaměstnanci v Americkém Námořnictvu si položili otázku, zdali je možné surfovat po internetu bez znalosti toho kdo je kdo. Přišli tak s teoretickým

Onion routingem. V roce 2000 pak Paul společně Rogerem Dingledinem, studentem v MIT, začali pracovat na první verzi TOR sítě a proxy, která by uživatele připojila k síti. Ta vyšla v roce 2002 jako open-source. Prohlížeč však vznikl až v roce 2008.

K čemu to tedy všechno bylo?! Zpoza TORu se dostanete k webovým stránkám, které jinak nejsou dohledatelné. Většina těchto webových stránek je svým obsahem nechutná a nelegální. Jedná se o všechny typy pornografie, obchody s drogami, různými nabídkami na kybernetické útoky, vraždy a prodejem zbraní z černého trhu. Většina z toho jsou podvody, krom obchodu s drogami, který svou podstatou závisí na dlouhodobých klientech, a tak se většinou jedná o opravdový produkt, který nechce zákazníka pouze okrást. K transportu peněž se pak nejčastěji používají kryptoměny, které jsou hůře vystopovatelné.

K čemu je to dobré?! Dark web má i světlou stránku. Umožňuje lidem v censurovaných zemí vynášet informace o tom co se v zemi děje a dostávat informace ze světa.

Software

„Nevidíme daleko do budoucnosti, ale stejně před sebou zříme hromadu věcí, které je třeba udělat.“

- **Alan Turing, Computing Machinery and Intelligence (1950)**

Každý den používáme elektronická zařízení. Od mobilních telefonů přes kreditní karty až po počítače. Denně se jedná o jednoduchou činnost, kterou se je schopné po chvíli naučit i dítě. Ale co kdyby tomu tak nebylo? Co kdybychom pro odeslání emailu museli vymyslet zapojení 20 kabelů? Naštěstí toto není realitou. Dříve když byly počítače ještě v plenkách, byla veškerá logika dělána lidmi a počítač pak pouze vypočítal daný úkon. S vývojem se však počítače vyvinuli a vývojáři a programátoři potřebovali myslet méně o fyzičnu a více o teorii s počítači spjatou. Abstraktní vrstvě, která běží na počítačích se tak říká

software. V následující kapitole si ukážeme dvě základní témata v oblasti softwaru. Zcela jistě to není ani kousek toho co se opravdu řeší v reálném světě, ale nastíní to některé problematiky, které denně využíváte a nemusíte si toho být vědomi.

Ještě, než začnu tak je potřeba říci, že počítač v teorii dělíme na několik vrstev. Software je abstraktní část. Hardware je část fyzických komponentů. A operační systém je něco, co tyto dvě části spojuje.

Operační systém (OS)

Je vrstva počítače, která spojuje všechny programy, aplikace a služby s hardwarem. Říká hardwaru, co má zrovna vypočítat, uložit či načíst a jakému programu to poslat. Samotný operační systém je pak uložen na disku a je spuštěn BIOSem. Ten je předinstalovaný na mateřské desce vašeho počítače. OS běží na určité architektuře procesoru. To následně ovlivňuje i jaké aplikace na tomto počítači budou moci běžet. Byť se již většina programů a systémů vytváří na všechny architektury je toto třeba vzít v potaz, když se budete snažit instalovat OS pro ARM na x86 procesor. Pro představu moderní procesory série M od Applu jsou ARM, kdežto většina procesorů Intel je x86. Podíváme se na historii některých z nich.

Unix – 1969

Unics jak se tehdy jmenoval, vznikl jako reakce na vývoj několika jiných operačních systémů tehdejší doby. Na vývoji se podíleli MIT s AT&T, hlavními vývojáři pak byli Dennis Ritchie a Ken Thompson. Původně se mělo jednat o přívětiví operační systém pro testování programů, který není přenositelný na jiné počítače ani nepodporuje běh vícero programů. V roce 1973 byl však přepsán do jazyka C. Což z něj učinilo kompatibilní operační systém pro mnoho počítačů a v 70‘ letech se tak rozšířil do mnoha univerzit. Díky některým funkcím jako je řetězení výstupů programů jako vstupu do dalších programů, se stal velice populárním a používaným. V roce 1980 pak Microsoft udělal operační systém Xenix, který je založen na Unixu. Stejně tak i BSD, který inspiruje další rodinu operačních systémů. V následujících letech se tak z něj stává jakýsi základ pro operační systémy. Dnes by se dal považovat za jeden z nejvýznamnějších, ne-li ten nejvýznamnější operační systém vůbec. Nutno dodat že tehdy ještě neexistoval GUI. Neboli Graphical User Interface. Vše se tak odehrávalo v terminálu.

Xerox ALTO – 1973

Byl jeden z prvních počítačů, který měl ve svém operačním systému, uživatelské rozhraní. V roce 1979

vyměnil Steve Jobs okolo jednoho milionu dolarů v akciích za návštěvu výrobny těchto počítačů. Tehdy šlo už o nový model, i tak ale inspiroval Jobse k tvorbě Lisy. Počítače s operačním systémem, který měl plně funkční GUI tak jak jej známe dnes.

MS-DOS – 1981

Microsoft DOS byl druhý operační systém od Microsoftu, který se později prodával zároveň s Xenixem. Zatímco ten byl určen pro náročné uživatele. MS-DOS byl určen pro veřejnost. Vznikl pro počítače IBM, které CP/M odmítl vybavovat unikátním systémem. Bill Gates tak koupil počítač DOS a s jedním z jeho tvůrců Timem Patersonem, jej upravily a produkovali jako MS-DOS. IBM však získalo pouze licenci a nebyli jediným odběratelem.

GNU – 1983

Vytvořil **Richard Stallman** jako odezvu na UNIX, který se v mezičase snažil AT&T komerčně prodávat. GNU neboli „GNU není UNIX“ má být veřejně dostupný a zdarma napsaný operační systém. Pracovalo se na něm přes celá 80‘ léta a jediné co v roce 1990 zbývalo bylo jádro. S tím přišel nezávisle Linus Torvalds (viz. Linux - 1991).

Lisa a Apple – 1983

Lisa byl jeden z nejvýznamnějších počítačů od Applu, a údajně se jmenovala po dceři Steva Jobse. Jeho operační systém Lisa OS byla jeden z prvních, který nabízel úplné uživatelské rozhraní. V kombinaci s aplikacemi jako je malování, tak ovládání zvládli i malé děti. Počítač byl velice úspěšný a zpopularizoval GUI pro širokou veřejnost. Později se z operační systém přejmenoval na Mac OS. Paralelně však po návratu Jobse do Applu v roce 1997 vznikl nový operační systém, který se jmenoval Mac OS X. A byl založen na kompletně jiném principu, než tento původní „klasický“. Ten zanikl v roce 2001 s vydáním Mac OS 9, které nabádalo uživatele na přechod do nový systém. Dnes všechny počítače od Applu mají v sobě Mac OS X, který se dnes paradoxně označuje opět pouze jako MacOS. V roce 2007 pak Apple představil svůj Iphone, který používá za svůj operační systém IOS. To je pouze zmenšenou verzí počítačového systému. Na svou dobu byl však revoluční právě v operačním sytému, který je jednoduchý a dobře ovladatelný uživatelem oproti konkurenci, který zaostávala. Jako odezvu na Apple přišel Google se svým Androidem (Viz. Android - 2008).

Unixové války – 1984

Po úspěšném vytvoření UNIXu se spousta organizací podílela na vývoji vlastních komerčních a nekomerčních verzích tohoto systému. Primárně byla tak oficiální verze od firmy AT&T, která UNIX vytvořila. Z této větve později pak vznikl i Solaris od Oraclu. Další byla rodina BSD systémů, která vznikala na Kalifornské univerzitě v Berkley (Berkley Software Distribution).

V roce 1984 vznikla skupina Open Group for Unix Systems (X/Open) s několika menších firem pracujících na vlastních verzích Unixu. Tato skupina si byla vědoma mnoha různých distribucí tohoto softwaru a jejich nekompatibility mezi sebou samými navzájem. To chtěla změnit vytvořením jediné organizace určující standardy pro UNIX. AT&T účast v této skupině odmítla, neboť si myslela, že jako mateřská spolčenost UNIXU by měla také standardy určovat ona. To a další společné zájmy vedli v roce 1987 ke kooperaci AT&T se společností Microsystems, která až do té doby vydávala verze BSD systémů. Tato aliance byla pro obě společnosti výhodná a navzájem měla utvářet jakýsi monopol. Pro ostatní firmy už tolik ne. Vedla k vytvoření Open Software Foundation, která byla tvořená z dalších firem spojených v odporu vůči monopolu, který vznikal u AT&T. Nakonec se OSF

podařilo přesvědčit k připojení největšího oponenta AT&T a to IBM. Což vedlo k masivnímu připojování se firem k jedné z těchto stran. OSF se snažila AT&T přemluvit k připojení, dokonce s nabídkou že se vývojem standardů začne na nové verzi systému od AT&T, ale podmínkou bylo že se na vývoji budou podílet všechny členské společnosti, což se korporátu nelíbilo. Unie mezi AT&T a Microsystems se následně přejmenovala na Unix International v roce 1988.

Tyto války o standardizaci UNIXu vedli v roce 1993 k otevření díry na trhu, který vyplnil Windows NT od Microsoftu, který se později vyvinul ve Windows Server. To vedlo obě skupiny k přehodnocení svého postavení a v roce 1994 se spojily pod označením The Open Group. V roce 1996 se k nim připojila i skupina X/Open. Dnes je tato skupina poskytuje oficiální standardy pro Unix. Nutno dodat GNU/Linux vyšel jako jedno z odvětví Unixu. A mnoho dalších distribucí není zdarma, jak je tomu třeba nutností u distribucí Linuxu.

Z Unixu vychází dnes systémy jako je FreeBSD, OpenBSD, MacOS (Původní), Solaris, GNU/Linux, NetBSD, AIX, HP-UX a další...

Windows – 1987

Microsoft jako reakci na zvětšující se popularitu GUI představil v roce 1987 svůj Windows 1.0. Zároveň s vývojem lepší technologie začal podporovat i multi-tasking. Programy se tak nemuseli zavírat, aby se otevřeli další. Windows dostal své pojmenování podle typu GUI, které používal. Okna (z angl. window) jsou jednotlivé aplikace běžící na systému. Společně s verzí 2.0 běželi na MS-DOS. Třetí verze už konkurovala Applu, ale ještě jej nepředčila. Verze 3.1 pak byla přeložena i do češtiny. Opravdová revoluce přišla až v roce 1995. Tehdy vyšel Windows 95, který vylepšil uživatelské rozhraní a přinesl plochu tak jak ji známe dnes. Stal se komerčním úspěchem a po dlouhé době předčil i Apple. V roce 2001 pak přišel Windows XP a v roce 2007 Windows Vista. O dva roky později pak Windows 7, který byl až do roku 2019 nejpoužívanější operační systém na světě. Přinášel některé funkce jako je ovládací centrum a další vylepšení. Moderní verzí měl být Windows 8. Ten byl dokonce vyvinut i jako první systém od Microsoftu na procesory architektury ARM. Nebyl ale přespříliš populární. V roce 2015 vyšel Windows 10 a v roce 2021 Windows 11. Při vydání Windows 11 byly zpochybňováni některé nároky a na instalaci tohoto operačního systému, který vyžaduje Secure Boot a TPM 2.0.

Linux – 1991

Linus Torvalds byl finský student na univerzitě v Helsinkách. V roce 1991 začal pracovat na vlastním kernelovém jádru pro počítače PC AT od IBM. Původně se toto jádro mělo jmenovat Freax, protože Linux jako kombinace jmen Linus a Unix zněla až moc egoisticky. Ale vlastník FTP serveru, kde byl kód zavěšen a Linusův přítel se rozhodl mu složku přejmenovat opět na Linux. V roce 1992 se po zvažování rozhodl zveřejnit Linux pod GNU open-source licencí, která jej zpřístupnila celému světu. V kombinaci s projektem GNU tak tvořil plnohodnotný operační systém. GNU/Linux jak by se měl správně označovat (dle některých názorů, význam GNU pro Linuxové jádro je otázkou spousty hádek) je kompletně transparentní a dohledatelný na internetu. Zároveň pohání většinu serverů na celém světě. Operační systém pak začal mít vlastní distribuce (variace). Každý uživatel a vývojář který si chtěl OS přizpůsobit, upravit, vylepšit tak mohl zcela kompletně udělat. Pod podmínkou že jeho verze bude mít veřejně dohledatelný a přístupný zdroj (open-source). Dnes máme stovky, ne-li tisíce distribucí, které se větví jako strom. Mezi ty hlavní patří Debian, Redhat, Slackware, CentOS, Fedoraß, Ubuntu, OpenSuse a mnoho dalších....

Každý uživatel si tak může vybrat vlastní distribuci podle svých preferencí. Každý by měla být veřejně a zdarma dostupná. Některé, zejména ty z větve Redhatu však svou licenci GNU obcházejí a byť svůj produkt zpřístupňují zdarma. Účtují si za koncovou služby u větších zákazníků.

Dokonce Windows po letech váhání začal s Linuxem spolupracovat. A pokud jste uživatel Windowsu můžete si stáhnout aplikaci WSL (Windows Subsystem for Linux), který vám umožňuje běžet Linux na Windowsových strojích. Toho samého výsledku můžete dosáhnout přes virtualizaci skrz aplikace jako je WMware či Oracle VirtualBox. Nebo můžete kompletně přeinstalovat svůj operační systém na jednu z Linuxových distribucí. Dnes je instalace velice snadná a na internetu lze dohledat jednoduché návody. V takém případě se doporučuje používat nějakou jednoduší distribuci pro nové uživatele jako je například Xubuntu.

Android – 2008

V roce 2008 vyšel Android, založený na GNU/Linuxu. Firma existovala už od roku 2003 a měla se zabývat operačními systémy pro digitální kamery. V roce 2005 byla odkoupena Googlem a začala vyvíjet vlastní operační systém pro chytré telefony. Když v roce 2007

vyšel IPhone se svým IOS bylo jasné, že na trhu bude poptávka po konkurenci. Tuto roli obsadil právě Android v roce 2008. Zprvu byl na mobilních telefonech od značek jako je Motorola a HTC. Zprvu nebyl příliš úspěšný, ale po dobrém implementování služeb, které poskytoval Google, jako je YouTube, Maps a Chrome se stal velice populární. Od té doby se pravidelně vydávají nové vylepšené verze vždy s přezdívkou po nějakém cukroví. Například verze 1.6 je pojmenovaná Donut, a 2.3 je perníček (Gingerbread). Letos v roce 2024 vyšla již verze Android 15 s interním pojmenováním vanilková zmrzlina. Dnes se odhaduje že je android na více než 70 % všech chytrých telefonů na světě. Za jeho úspěchem nepochybně stojí i možnost distribuce systému mezi vícero výrobců mobilních telefonů, než je tomu u Applu a jeho IOS.

Programovací jazyky

Když máme funkční aplikace a operační systémy vyčnívá otázka, jak taký produkt vytvoříme. Předtím než bylo programování, existovali algoritmy („recepty“) jak udělat jistý úkon. Za programování by se pak dalo považovat nastavení počítače, tak aby taký úkon udělal. Zprvu se to dělalo čistě manuálně a odtud se berou historické „programovací“ šicí stroje a další

obdobné fyzické programování. Potom co proběhla počítačová revoluce včele s Alanem Turingem začalo být programování více o elektronických úkonech, jak ukládat a pracovat s daty na počítači. Dnes programátoři vytvářejí a vyvíjí aplikace, programy a systémy na míru pro širokou škálu různě náročných uživatelů.

Assembly Language – 1949

Je jeden z prvních programovacích jazyků na počítači vůbec. Historicky jej předčil pouze Plankalkul, který dokázal z paměti vyvolávat některé uložené kódy a matematické postupy. Assembly má několik desítek typů operací, které počítači říkají, co má udělat. ADD například říká ať počítač přesune hodnotu jednoho parametru do druhého. AND říká počítači ať udělá logickou operaci konjuknce mezi prvním a druhým parametrem.

Dnes máme několik typů Assembly a vždy se liší podle typu procesoru, na který program vyvíjíme. Máme tak ARM, X86, MIPS a další ... dá se tak říci, že tento programovací jazyk je jeden z nejnižších, co máme a fakticky interaguje přímo s hardwarem.

Při **kompilaci** programu, tedy převedení zdrojového (čitelného) do binární (spustitelné) formy. Je

mezikrokem právě převedení do Assembly typu daného procesoru. **Dekompilace** je proces opačný a snaží převést binární program do zdrojového kódu. To se dělá pomocí aplikací jako je Ghydra (původně od NSA) nemá to však kompletní úspěšnost, a tak je občas výhodnější zobrazit si právě mezikrok v Assembly.

Fortran – 1957

Formula **Tran**slator byl jazyk, který nastolil jistý abstraktní standard dalším budoucím programovacím jazykům. Místo přímých instrukcí byl jazyk už více abstraktní a fungoval jako nadstavba pro strojový kód. Uživatele a programátoři tak nemuseli přemýšlet, jak převést žádanou funkci do jednotlivých instrukcích, ale mohli tvořit zdrojový kód, který se pak do strojového převede.

Fortran se používá dodnes, kvůli svému rychlému výkonu a větší přístupnosti oproti Assembly se používá při programování superpočítačů. Stále se jedná o jeden z nejrychlejší programovacích jazyků při práci s matematickými úlohami.

COBOL – 1959

COBOL je programovací jazyk na němž v roce 1997 běžel 80 % světového kódu. Jedná se o jazyk, který se svou syntaxí podobá až moc anglickému jazyku. Bylo to tak schválně zamýšleno, neboť komise, která byla v roce 1960 sestavena za účelem vytvoření tohoto jazyka, primárně cílila na manažery a vedoucí funkce. Komisi byla vytvořena v rámci konference, která se konala o rok dříve v USA. Ta spojovala představitele firem a státních i nestátních institucí za účelem vytvořit standard pro programovací jazyk. Vznikl právě COBOL, který zavedl různá klíčová slova, odstavce, sloupce a další nápady, které se implementovali i v pozdějších jazycích. Jazyk se dodnes používá v systémech, které si nemohou dovolit jej vyměnit či zastavit provoz.

BASIC – 1964

Vytvořen původně jako úvodní jazyk pro studenty a podniky, které se chtěli do programování teprve dostat. Následně by přešli na těžší jazyk jako je Fortran. V osmdesátých letech se tohoto jazyka chytil Bill Gates a Paul Allen, kteří jej zpřístupnili pro počítače Altair a později i pro počítače od Applu a DOS od IBM. Následně dal vzniku i Visual Basic od Microsoftu v roce 1991 a .NETu (2001), který z BASICu také vychází.

Popularitě tomuto jazyku pomohlo primárně rozšíření na malé počítače, díky čemuž vznikali i aplikace pro malé firmy.

PASCAL – 1970

Pascal byl stejně jako BASIC vytvořen jako výukový programovací jazyk. Stalo se tak ve švýcarském Curychu profesorem Niklausem Wirthem. Je pojmenován po známém matematiku Blaisu Pascalovi. Obsahoval čtyři datové typy a to číslo, číslo s plovoucí čárkou, hodnotu pravdu/nepravdu (0 či 1), charakter (př. ‚a'). Jeho kompilátory se rychle rozšířili po vysoké škále procesorů a počítačů. Mezi ty známější procesory patří například Intel 8088. Ovlivnil pak hlavně jazyky jako je C. Dnes se už tolik nepoužívá.

C – 1972

Je jeden z nejznámějších programovacích jazyků k dnešnímu dni. Vytvořil jej Dennis Ritchie, který se později podílel na tvorbě Unixu, ten právě pak celý přepsal právě v jazyce C. I to pravděpodobně napomohlo k rozšíření jazyka C. Právě tvorba Unixu vedla ke vzniku C. Po verzi s PDP-7 assemblerem a fortranem přišli s návrhem vytvořit vlastní programovací jazyk. První Thompson (jeden z autorů Unixu) vytvořil jazyk B. Z něho pak vznikl jazyk C.

Z jazyka C vznikla pak celá škála dalších jazyků a programů. Dnes se jedná o jakýsi standard. Ritchie spolu s Brianem Kernighanem pak vydali knihu o jazyce C. Ta je dodnes vydávána a slouží jako výtečná učebnice tohoto jazyka.

SQL – 1972

SQL **není programovací jazyk.** Tak proč tady je tedy zmíněný? Structured Query Language je jazyk vytvořený pro ukládání, získávání, měnění a další práci s daty v databázi. A co je to Databáze? Jedná se v principu o soubor s velkou velikostí, jehož cílem je uložit a utřídit zadaná data. V databázích tak může být uloženo jméno zaměstnance s jeho adresou, telefonním číslem. Zaměstnavatel pak při potřebě zavolat jednomu zaměstnanci vyhledá právě jeho kolonku v databázi a zobrazí si jeho telefonní číslo. To o databázích v teorii.

Původně se tento jazyk jmenoval Structured Query English Language (SEQUEL) a byl navrhnut v IBM Donaldem Chamberlinem a Raymondem Boycem. Pro komerční účely byl zveřejněn v roce 1979 a od té doby se stal standardem pro databáze. Oficiálně byl standardizován v roce 1987 americkým ANSI. Na původní SQL pak navázalo mnoho dalších variant jako je MySQL, MS SQL (Microsoft), Oracle SQL, T-SQL.

C++ - 1979

Obohacená verze jazyka C o Objektivně Orientované Programování (OOP). S tímto konceptem přišel Bjarne Stroustrup při práci pro Bell Labs. Programování se tak stalo více abstraktní a třídy umožňovali tvorbu objektů, což ještě více zvyšovalo možnosti programování, částečně na úkor rychlosti (u dalších programovacích jazyků). Původně se jazyk měl jmenovat C s objekty (C with Objects), ale následně bylo rozhodnuto že půjde o C++ což indikuje zvětšení hodnoty C o jednu, stejně jak je tomu v programování. V roce 1985 byl publikován do veřejnosti a o 4 roky později byl standardizován ANSI.

Celý jazyk pak prakticky nahradil klasické C a dnes je jeden nejpoužívanějších programovacích jazyků vůbec. Jsou v něm vyvíjeny operační systémy, programy a aplikace.

Karel – 1981

V roce 1981 vydal Rich Pattis programovací jazyk Karel. Jmenuje se tak protože referencuje na Karla Čapka, autora slova Robot. Jedná se o jednoduchý jazyk, který má vysvětlit základy programování těm nejmenším programátorům (dětem). Píšete instrukce robůtkovi, který se pohybuje podle vašich pokynů a kreslí tak

obrázek. Účelem jazyka tak nebylo vytvořit žádnou aplikaci, ale naučit malé ratolesti, logice a zábavě v programování. Celý jazyk byl vytvořen v Pascalu.

Perl – 1987

Napsaný v jazyce C programátorem Larrym Wallem, který pracoval jako systémový administrátor pro NASU, je jeden z mladších tradičních programovacích jazyků. V podstatě vznikl, protože jeho autor byl na pomezí kdy úkon, který od počítače potřeboval byl příliš složitý na skriptovací bash jazyk. Ale on sám byl pak příliš líný na sepsání programu v jazyce C. A tak vznikl Perl. Jazyk napsaný v jiném jazyce pro zjednodušení některých úkonů.

Perl pak dostal další šanci při vzniku World Wide Webu, ale brzy jej nahradil PHP. Jazyk se tak dnes moc nepoužívá, ale má stálou komunitu, která jej stále podporuje.

Python – 1991

Znamená krajta, ale je pojmenovaný po britské komedii od BBC, Monty Pythonu. Vytvořen Guidom van Rossumem je po stránce syntaxe jeden z nejpřívětivějších jazyků dnes. Většina programovacích jazyků je složitějšího a „ukecanějšího“ rázů. To přesně python není. Je velice

snadný a při tom efektivní. Mohou se jej tak naučit i lidé, kteří s programováním teprve začínají a po chvíli budou mít hned první výsledky. Jedinou nevýhodou tohoto jazyka je jeho čas kompilace. Který je jeden z pomalejších oproti konkurenci. I tak je jazyk populární pro práci s velkými daty a pro počítání matematické úkony.

Ruby – 1993

Moto tohoto programovacího jazyku je, že je přirozený ne snadný. Jeho autor Yukihiro Matsumoto jej vytvořil jako kombinaci jeho oblíbených programovacích jazyků Perl, SmallTalk, Eiffel, Ada, Lisp. Cílem tohoto programovacího jazyka bylo vybalancovat mezi funkcionálním a imperativním programováním. Větší popularitě se mu dostalo až v roce 2006.

Brainfuck - 1993

Vznikl ve Švýcarsku jako ezoterický programovací jazyk. Co to vlastně znamená? Tento jazyk je v praxi absolutně nepraktický. Napsat v něm jakýkoliv program je pro vás, jak již jeho název napovídá absolutní bolest hlavy. Nicméně to dokáže. Vytvořil jej Urban Müller a skládá se pouze se znamének +-<>[],.#! . Jazyk se přirozeně nepoužívá, i tak máte-li příliš

volného času a dobré nálady, můžete si zkusit něco v tomto jazyce napsat.

Java – 1995

Jmenuje se po ostrovu v Indonésii, kde vznikla jedna z prvních káv. Tehdy to bylo zřejmě populární slovo, neboť se po něm pojmenoval ještě JavaScript. Java byl OOP jazyk pro vývoj aplikací a programů. Stal se velice populárním pro vývoj napříč platformami, neboť jej šlo zkompilovat prakticky kdekoliv. Především na androidech což zapříčinilo jeho popularitu zvláště mezi uživateli vývojáři pro chytré telefony.

Původně jazyk vytvořily James Gosling, Mike Sheridan a Patrick Naughton ve společnosti Sun Microsystems, což byla dceřiná společnost Oracle. Celý jazyk měl být bezpečný, výkonný, objektivně-orientovaný, interpretovaný a dynamický. Stejně tak jak dlouhý je jeho popis je i jeho syntaxe. Jazyk je poměrně ukecaný na druhou stránku není přespříliš chybový a uživatele tak častokrát sám opraví. Celý jazyk pak inspiroval Microsoft při vývoji své obdoby C#.

PHP – 1995

Byl vytvořen krátce po vzniku a růstu World Wide Webu. Navrhl jej Rasmus Lerdorf pro osobní účely sledování provozu jeho osobních stránek, ale nakonec

celý projekt přerostl v jazyk, který měl na starost práci s webovými stránkami na serveru. Možnosti jako databáze a interakce stránky s počítačem se stali zajímavými pro vývojáře. PHP se dodnes používá jako takzvaný Back-endový jazyk. Neboli jazyk, který komunikuje mezi webovou stránkou a serverem, kde tato stránka běží. Dodnes absolutní většina stránek běží právě na PHP. Byť v něm byly nalezeny bezpečnostní chyby a při špatné implementaci hrozí snadný útok na server.

C# - 2000

Jazyk od Microsoftu běžící na frameworku .NET, který se podobá kombinaci C++ a Javy. V tomto jazyce je naprogramovaný například známý herní engine Unity. Kvůli němu se stal jazyk populární i při vývoji her. Dále se používá pro tvorbu windowsovských, mobilních a webových aplikacích. Často se pak používá při výuce ve školách a jako úvodní jazyk pro začátečníky. Je jeden z mála progresivních jazyků, který se stále snaží implementovat nové věci.

Go – 2007

Vznikl ve společnosti Google jako žádost vývojářů na některé problémy s ostatními jazyky. Jedná se open-sourcový projekt, který cílí na velká data, sítě a toky.

V podstatě na všechno, s čím se Google potýká. Jeho hlavním maskotem je modrý pytlonoš, což je druh hlodavce podobný syslovi.

Swift – 2014

Swift vznikl uvnitř Applu jako řešení pro vývoj na jejich vlastní produkty. Do té doby byli všechny aplikace tvořeny v C, C++, a Objektivním C. Chris Lattner vedl vývoj tohoto jazyku a dnes je jazyk i kompilátor open-source. Po chtěné modernizaci jazyka vznikl jako syntaktická kombinace Kotlinu, Javy, C jazyků. Jeho hlavním editorem je Xcode, ale přirozeně dá vyvíjet v jakémkoliv jiném programovacím editoru (IDE). Je-li vaším cílovou platformou IOS, MacOS či jiné Apple produkty, pravděpodobně použijete Swift.

Rust – 2015

Graydon Hore, zaměstnanec pro Mozillu, vymyslel tento jazyk jako náhradu místo jazyka C/C++ poté co v roce 2006 nefungoval jeho výtah domů a on musel vyjít 21 pater do svého bytu. Jazyk, jehož hlavním účelem je práce s pamětí se stal velice populární a dnes je jeden z nejpoužívanějších na světě. Svou rychlostí pak překonal i původní jazyk C. Projekt od roku 2009 sponzorovala Mozilla. Jeho první verze byla

pak vydána v roce 2015. Dnes již existuje Rust Foundation, která má za cíl Rust rozvíjet a vyvíjet.

Zig – 2016

Je jeden z nejmladších programovacích jazyků. Zatím se jedná o malý projekt, který dosahuje výkonných výsledků v porovnání s ostatními jazyky. Uvidíme, co se z tohoto projektu do budoucna vyvine.

Kybernetická bezpečnost

„Technika nezná Hippokratovu přísahu.“

- **Edward Snowden, Nesmazatelné záznamy**

Kybernetická bezpečnost je dnes obrovským tématem, které se řeší ve státních i soukromých sektorech. Proč se jedná o tak velké téma? Odpověď je docela prostá. S vývojem internetu a technologií, které jsme si již prošli, bylo jen otázkou času, než se najde někdo, kdo tyto technologie zneužije ke svému prospěchu. Vznikly tak první hacky a hackeři. Podíváme se na nejdůležitější události, technologie a tvůrce provázející toto odvětví, kteří nás dovedli do situace, v níž jsme dnes. Častokrát není kybernetická bezpečnost jenom o technologii – jen o svobodě, informacích, sdílení technologií a pravdy – a proto vše co zde je napsáno, nemusí být čistě technologického rázu. Úvodem je dobré zmínit definici dvou důležitých slov

Hack

Má obecně dvě významy. Tradičně se jedná o vniknutí do cizího počítače bez vědomí vlastníka. K tomu mohou být použity digitální či fyzické pomůcky. Druhá definice tvrdí že se jedná o podařené, nápadité či důmyslné řešení problému počítačové aplikace způsobem, který autor nezamýšlel. Veřejnost většinou obecně považuje hack za jakýsi nelegální akt, který z jeho autora činí zločince. Nemusí tomu tak ale vždy být.

Hacker

Je osoba, která provádí hack. Často je asociovaná s nelegální činností a obecně je v lidech zakořeněno, že je takovýto člověk zločinec. Pravdou je, že hackery dělíme na několik typů. Většinou se označují podle barvy čepice (v angličtině ‚hat'). White hat hacker je tak legální tester, který zkouší bezpečnost webu, serveru, aplikace za určitou odměnu. Black hat hacker je naopak ten, kdo zneužívá zranitelností v těchto systémech pro svůj vlastní prospěch. Grey hat hacker je pak něco mezi těmito dvěma. Přirozeně je mnoho dalších barev, které nejsou vždy uznávané komunitou, ale obecně platí, že hacker není vždy zločinec.

Historie

V celé kapitole se podíváme na lidi, události a v podstatě vše významné, co ovlivnilo komunitu zabývající se bezpečností. Jak již bylo dříve zmíněno, jsou věci, které nejsou přímo historií tohoto oboru, ale ovlivnili jej natolik, že si je prostě musíme říci znovu a ukázat si co způsobily.

Kevin Mitnick – 1963

Kevin byl jeden z nejznámějších hackerů všech dob. Přesto činy však nejsou známé jako prolomení nejlepších softwarů své doby, ale jako využití sociálního inženýrství pro vlastní účely. Sociálním inženýrstvím je myšleno hacknutí člověka, tedy snaha docílit daného výsledku bez hledání slabin softwaru či technologie pomocí lží, manipulace a přesvědčování. Slabinou je v tomto případě člověk.

Mitnick byl tímto proslulý, ale samozřejmě měl i výborné znalosti a zkušenosti o technické části hackování. V 80. a 90. letech byl na listu nejhledanějších lidí FBI. Až do roku 1995 kdy byl dopaden po třech letech na útěku. V roce 1998 jej nakonec odsoudili na 46 měsíců ve vězení. Mezi těmito roky probíhala velká kampaň jeho příznivců s titulem

„Free Kevin“, neboli osvoboďte Kevina, která se objevila i na hacknutých stránkách Yahoo.

Po propuštění z vězení se stal bezpečnostním znalcem na problematiku počítačů. Založil vlastní firmu Mitnick Security a dlouho pracoval jako bezpečnostní konzultant pro mnoho největších firem světa. V roce 2023 zemřel na rakovinu slinivky. Vydal spoustu knihy, měl děti a je na něj vzpomínáno jako na jednoho z prvních hackerů své doby.

Čína – 1975

Zakladatel čínské lidové armády Ye Jianying podává zprávu pojmenovanou jako „Práce o posilování elektronických opatření“ v níž stojí návrhy jak by Čínská lidová osvobozenecká armáda, mohla využít moderní stroje k posílení síly své armády. Doufal, že by Čína v roce 2049, 100 let od založení Čínské lidové republiky, mohla předčít Spojené státy americké jako nová světová velmoc.

O pár let později se vedení ČLA tímto dokumentem opravdu začala řídit a zakládá vysoké školy pro výcvik svých vojáku v elektronickým boji. Elektronický boj mezi velmocemi světa a ostatními zeměmi se označuje jako „Cyberwarfare“ (V doslovném překladu „Kybernetická válka“). Ta se vede i dnes, naštěstí zatím

neeskalovala ve vyšší konflikt. Častými cíli těchto mezistátních útoků jsou informace, data a sabotáž.

Chaos Computer Club - 1981

Je hackerská skupina založená v německém Hamburgu. Začalo to několika přáteli, kteří se chtěli bavit o stavbě amatérských rádií, počítačů, kryptografii a dalších „šprtských“ tématech. Byli silně proti-autoritářští, což se stalo částečně i symbolem moderních undergroundových hackerů, kteří se CCC inspirovali.

V roce 1984 začaly první incidenty tohoto klubu. Nabourávali se do telefonní sítě s vlastním nástrojem, který pojmenovali „The Cat“, neboli kočka. V témže samém roce spáchali něco, co na světě nemělo obdoby. BTX stroje, byly tvořeny z klávesnice, televize, telefonu a fungovali jako modulární počítače. V té době se přes ně daly odesílat platby a poplatky. Klubu se pak podařilo získat heslo BTX stroje jedné z německých bank a na svůj účet si tak odeslali několik příspěvků. Jednalo se pravděpodobně o první digitální loupež banky v historii. Druhý den všechny příspěvky vrátili a upozornili na bezpečnostní chyby.

V CCC začínali i zakladatelé ART+COM, jejichž Terravision byl předchůdcem Google Maps. Jejich

příběh můžete znát z volné seriálové adaptace od Netflixu „Kód za miliardu dolarů“ (2021).

Dodnes je CCC velice aktivní a zabývá se hacktivismem, bojem za svobodu projevu a digitálními právy. CCC se rozšířilo do Berlína a má teď malé pobočky téměř po celém Německu.

Cult of The Dead Cow - 1984

Kult mrtvé krávy (cDc) byl americký undergroundový hackerský spolek, jehož cílem bylo vytvořit místo, kde by si hackeři mohli navzájem sdílet myšlenky, nástroje, tipy a doporučení. Patří mezi zakladatele Hacktivismu, což znamená že jejich činnost měla politický a sociální efekt. K bývalému členství v této skupině se hlásí spoustu významných Američanů, třeba i bývalí kongresman za Texas Beto O’Rourke.

V roce 1996 byla založena Ninja Strike Force, která jako větev této skupiny vykonávala útoky, které byly v souladu s cíli cDc. Podíleli se třeba na vývoji aplikací, které by Číňanům pomáhaly obejít jejich tvrdou cenzuru internetu. Pracovali na nich s čínskou skupinou „The Hong Kong Blondes“, neboli Hongkongské blondýnky. O rok dříve vyhlásili válku církvi Scientologie. Skupina je do jistý míry aktivní i dnes.

DEF CON - 1993

Měla být původně sraz několika lidí z jednoho hackerského fóra, které v těch letech fungovalo. Původně měl být sraz rozloučením se s komunitou, neb host webového serveru se stěhoval s rodinou a vědělo se, že fórum zanikne. Nakonec ale pozvali spoustu dalších lidí z jiných obdobných fór a vznikla z toho událost, která má jistotou podobnost například v kalifornském srazu hořícího muže. Celý sraz byl velkým úspěchem a začal se pravidelně obnovovat každý rok. Najdete zde spoustu „vesniček“ na specificky zaměřená témata hackingu.

V roce 1996 se zde uskutečnila soutěž mezi jeho členy, které se vyvinula až v dnešní soutěže Capture The Flag (CTF). Soutěže tohoto typu se rozšířily velmi rychle a staly se oblíbenými mezi středoškoláky, vysokoškoláky i veřejností. V dnešní době se běžně pořádají téměř každý víkend. Od roku 2015 se i v České republice koná celostátní kybersoutěž pro střední a vysoké školy, jejíž součástí je i CTF v druhém a třetím kole.

Deklarace – 1996

To byla reakce amerického básníka a bojovníka za svobodu na internetu Johna Perryho Barlowa na nový telekomunikační zákon schválený v USA. Konkrétně se

jednalo o deklaraci nezávilosti kyberprostoru. Stalo se to ve Švýcarsku v roce 1996. Říká v ní, že by žádný stát neměl určovat, co se bude s kyberprostorem dít - tedy v internetu a jakémkoliv dalším teoretickém počítačovém prostoru. Tato deklarace se stala jakýmsi krédem pro mnoho bojovníků za internetovou svobodu a nezávislost. Vystihuje i tehdejší pohled na internet jako nezávislý prostor, kde mohou lidé vystupovat zcela anonymně a vyslovovat své názory a myšlenky nezávisle na regulacích státu. V podstatě deklaruje kyberprostor jako vlastní entitu, nezávislou na státu. Samozřejmě váha takové deklarace je zpochybnitelná a stalo se tak ve všech regulacích států na světě. Přesto idea dodnes přežívá.

911 – 2001

9. září proběhl v roce 2001 útok na Světové obchodní centrum v New Yorku. Následně další letadlo zasáhlo americký Pentagon. Tato událost pohnula všemi Američany a tajné složky přiměla k akcím, které by jinak za normálních podmínek nebyly možné. Tajné složky začaly využívat chytrá zařízení od mobilů až po počítače pro sledování všech svých občanů. (viz sekce Občan čtyři)

Celá tragédie vedla k větším investicím do počítačových technologií a do bezpečnostních prvků

na všech státních i soukromých sektorech po celém světě. Pod záminkou boje proti terorismu se rozmohly aktivity, které nebyly vždy zcela legální.

4chan – 2003

Byl založen jako anglická náhrada japonského 2chan fóra. Od začátku bylo celé fórum anonymní a necenzurované, a i když se na něm prvně často vyskytovalo pouze anime a kresby jednotlivců, tak celá situace vy eskalovala ve fórum sdílející porno, vraždy a další nemilá překvapení. Jedna ze skupin, která se dala na tomto fóru dohromady byl Anonymous.

Anonymous – 2003

Skupina, která začala jako internetoví trollové v 4chanu se vyvinula v jeden z největších mezinárodních hackerských skupin k dnešnímu dni. Začínali jako skupina nájezdníku online her, jejichž jediným cílem bylo spáchat co největší neplechu v dané hře, na daném serveru. Později si však zadali ještě větší cíle. Místo provokování začali útočit na reálné organizace a firmy. V roce 2008 zaútočily na církev Scientologie, obdobně jako cDc před nimi.

Pirate Bay – 2003

Ve Švédsku založily Fredrik Neij, Gottfrid Svartholm a Peter Sunde webovou stránku, která fungovala jako prostor pro sdílení souborů mezi uživateli. Pro stáhnutí souboru se první musí stáhnout Torrent soubor, který funguje jako přímý odkaz na adresu daného souboru na internetu. Následně se stáhne daný soubor z internetu. Tento přístup naplňuje podmínky peer-to-peer (komunikace je čistě mezi dvěma uživateli, klient-ke-klientu).

Obsahem webu se však staly primárně „pirátěné“ filmy, hry a další soubory s autorskými právy. Proto na stahování a šíření takovýchto souborů bylo z pozice práva nahlíženo jako na krádež a porušení dalších zákonů. V České republice si vybavíte například web ulož.to, které fungovalo podobně, ovšem s tím rozdílem, že byly soubory uloženy na serverech webu, nikoliv u vás.

Zvláště USA mělo velký zájem na stažení tohoto webu a obvinění vlastníků. Chytit autory se jim v roce 2008 podařilo. Všem byl dán trest jednoho roku vězení a téměř 3 milionová pokuta v amerických dolarech. Po odvolání se trest stáhl o půl roku, ovšem pokuta se zvýšila téměř dvojnásobně. Web ovšem díky internetu přežívá dodnes.

WikiLeaks – 2006

Webová stránka sloužící jako azyl pro tajné dokumenty, nepohodlné soubory a data vyzrazené na veřejnost jednotlivci, byla založena v roce 2006 Julianem Assangem. Pravidelně čelí spoustě žalobám a soudním přím. Výrazně se však osvědčila jako platforma, kde mohou být pravdivé informace šířený bez ohledu na aktuální politické názory v zemi.

LulzSec – 2011

Hackerská skupina bývalých členů Anonymous podniká útoky převážně proto, že jim to připadá vtipné. Jeden z největších útoků LulzSecu je na účty Playstation Network, kde bylo odcizeno přes milión účtů. Celá skupina je známá především svými typickými SQL injection útoky, kdy se odešle požadavek do databáze oběti a ta se následně chová jinak, než bylo původně zamýšleno. Mezi jejich oběti patří především velké společnosti a státní složky. Ne vždy však svých činů zneužijí a v případě Britské zdravotní organizace dokonce upozornily administrátory na bezpečnostní chyby.

Silk Road – 2011

Digitální černý trh pro správné kupce. I tak by se dalo popsat fungování tohoto webu, který byl přístupný pouze skrze TOR. Jeho autor Ross W. Ulbricht jej provozoval mezi roky 2011 a 2013. Hlavními předměty prodeje byly drogy, zbraně, vraždy, hackerské útoky a pornografie, bohužel i ta dětská. Většina prodejců však slibovala hory a doly, ale po zaplacení kupcem, se prodejce vytratil. Přirozeně všechny transakce probíhali skrze kryptoměny. Ulbricht měl ze všech transakcí podíl, a tak vydělal velké množství peněž.

V roce 2013 na Ulbrichta proběhla policejní razie. Předcházelo jí dlouhé vyšetřování, které našlo na Ulbrichtově LinkedIn profilu zmínku o provozu multimilionové nelegální tržiště, mimo jiné další chyby, které vedly k jeho zatčení. Ulbricht byl v lednu roku 2025 propuštěn na pardon prezidenta Donalda Trumpu. Byl původně odsouzen na dvě doživotí a 40 let k tomu. Navíc mu byla zabavena většina peněz z jeho nelegálního podnikání. Nic však nepomohlo tomu, aby po vypnutí webu, nevznikly nové další varianty podobných trhů.

Občan čtyři – 2013

Edward Snowden se narodil v roce 1983 v Americe. Jeho rodiče byli vojenští zaměstnanci a on vyrůstal jako hrdý Američan. Od mala měl velkou náklonost k počítačům, která se rozšiřovala od hraní her do základů programování. Tehdy byla komunita internetu velmi přívětivá a on se nevědomky naučil hledat a zneužívat v počítačových i reálných systémech chyby. Měl tak ideální předpoklady pro to stát se hackerem. O tom dokonce vypovídá jím nalezená zranitelnost na webových stránkách Los Alamos, středisku jaderného výzkumu. Ta mohla vést k zveřejnění osobních údajů zaměstnanců a dalších citlivějších dokumentů. Tehdy třináctiletý Ed nejprve napsal email a následně zavolal přímo do střediska. Následně mu bylo poděkováno a nabídnuto místo zaměstnance. Musel bohužel pozici odmítnout, neboť mu bylo třináct a měl povinou školní docházku. Po útocích 11. září 2001 se rozhodl narukovat do armády, ale po zranění byl vyřazen.

Následovala kariéra kontraktora u CIA a NSA. Dvou tajných služeb, které po útocích 11. září drasticky rozšířili své pravomoci a cíle. Po cestách, jež obsahovali švýcarskou Ženevu a Hawaii se rozhodl odhalit tajemství, které všechny tajné služby skrývali. A to že špehovali nejen podezřelé osoby na světě, ale

všechny osoby. A to bez povolení soudu. Tomuto odhalení předcházelo spoustu příprav. Primárně sběř důležitých dokumentů, které by uváděli souvislosti a vysvětlovali technologii sledování občanů. Také bylo potřeba bezpečně komunikovat s novináři, kteří by měli vůbec zájem tento příběh publikovat. Neboť většina médii jde v těchto věcech státu vstříc.

Nakonec musel Snowden uniknout ze země. Články a videozáznam se natočil v Hongkongu, pak měl odcestovat do Ekvádoru, načež mu bylo vydáno i výjimečné povolení, avšak po příletu na mezipřistání v Rusku mu byl zablokován pas americkými úřady. Rusko mu však nabídlo azyl, který neochotně, ale z nutnosti přijal. Žije tam dodnes.

Proč se však za své činy spravedlivě nevydal? To je otázka americké spravedlnosti. Až moc lidí věří v dokonalost amerického systému, aby si uvědomila že i on má své chyby a cesty, jak jej zneužít. Snowden je přesvědčen o tom, že by se mu v Americe nedostalo spravedlivého soudu. A že většina Evropských států by přistoupila k extradici. Celý tento případ nás učí o důležitosti soukromí, a ne pouze jako nutného základního lidského práva, ale i o potřebě za tuto svobodu bojovat a hýčkat si ji. Kybernetická bezpečnost není vždy pouze o tom, jak zabezpečit či

prolomit systém. Ale i o tom jaká data bráníme a jaká data chceme od druhých získat. To vedlo i další organizace jako je Evropská Unie k vytvoření nových zákonů jako je GDPR.

CryptoLocker - 2013

Mezi lety 2013 a 2014 se po internetu rozšířil ransomware, což je typ programu, jehož účelem je zablokovat data uživatele a následně jej vydírat o peníze. Vyplatit chtěl v kryptoměně Bitcoin, která je obtížně dohledatelná, a tak zaručuje za jistých podmínek i částečnou anonymitu. Cílil na počítače s Windows operačními systémy a předpokládá se, že se rozšířil až mezi 34 000 počítačů v Anglicky mluvících zemích. Vydával se v emailech častokrát za zahraniční dopravní firmy FedEx a UPS.

Ukrajinské volby – 2014

Je prokázáno že jedna z proruských hackerských skupin CyberBerkut, pronikla 4 dny před začátkem voleb, do centrálního serveru voleb a chtěla ovlivnit výsledky. Ruská média dokonce zveřejnila výsledky voleb na Ukrajině dříve, než byli výsledky veřejné v samotné Ukrajině. Také se začalo více mluvit o Ruských dezinformačních kampaních po celém světě. Dnes žijeme v době, kde jsou tyto dezinformační

prostředky využívány, a tak radím čtenáři, aby si důležité informace ověřoval u autorit, které shledá za vhodné. To nechám na jeho svědomí.

GDPR – 2016

Evropská unie se rozhodla vytvořit zákon, který by ochraňoval data svých občanů na internetu. General Data Protection Regulation byl schválen roku 2016 a členské státy EU měli dva roky na jeho implementaci. Projednával se a v podstatě existoval od roku 1995, kdy existovala evropská směrnice 95/46/EC. Zákon prošel postupem času nějakými úpravami a stále se na něm pracuje.

Ve své podstatě zákon říká, jak mohou firmy a organizace na internetu spravovat vaše osobní data. Zkráceně by se dalo říci, že bez vašeho souhlasu to dělat nesmí. Problematika celého zákona je na dlouhé interpretování právníky, co vy z praxe můžete sledovat jsou „cookies“, sušenky, které na vás vybíhají na každém webu a ptají se vás, jak může web zacházet s vašimi daty. Většinou je předvyplněný tak, aby povolil všechno a očekává odkliknutí povolení. Tuto zákeřnou praktiku začali používat i nadnárodní firmy, které se této právní regulace poměrně štítí, neboť co si budeme obchod s daty uživatelů je výdělečná činnost.

Americké volby – 2016

Před začátkem voleb mezi Donaldem Trumpem a Hillery Clinton. Přišel phishingový email Johnu Podestovi, který předsedal komisi pro vedení kampaně Hillery Clintonové. Ten jej sice poslal na ověření, ale zaměstnanec udělal gramatickou chybku a na místo „nelegitimní“ napsal „legitimní“. Tímto způsobem se ruští hackeři dostali ke všem emailům související s kampaní demokratické strany. Později se objevily na WikiLeaks. Ruský prezident Vladimír Putin vyvrátil jakékoliv vazby na ruského hackera či hackerský tým, který měl tuto událost na starost. Později se však ukazují nové důkazy, které vypovídají o snaze zneužití těchto dat pro zvolení Republikánské strany a Donalda Trumpu. Mezi 5. a 6. lednem roku 2017 se po dlouhém vyšetřování sešli tajné složky s dosluhujícím prezidentem Obamou a nově zvoleným prezidentem Trumpem. Výsledkem jejich šetření bylo, že Rusko nikterak neovlivnilo samotné volební stroje či servery. Ale vedlo pomocnou kampaň, která byla silně podporovala republikánského kandidáta. V červnu téhož roku prezident Putin připustil, že by se mohlo jednat o útoky vedené občany ruské federace, ale že ruská vláda není nikterak zapojena. Později vychází najevo že hackeři cílily i na samotné výsledky voleb, jejich úspěch však není nikterak prokazatelný.

WannaCry – 2017

Obdobně jako CryptoLocker byl i tento program v kategorii ransomware. V květnu roku 2017 se začali objevovat jeho první výskyty, ale co na něm bylo výjimečného, je využití zero-day zranitelnosti, tedy takové, o které ani autor softwaru neví. Využíval chyby v Microsoft SMB. A cílil na počítače s operačními systémy typu Windows. Kvůli zranitelnosti se pak mohl šířit bez jakékoliv interakce s uživatelem. Program opětovně zašifroval, některé soubory a vyžadoval výpalné v kryptoměnách. Ve většině případů však k žádnému rozšifrování nedošlo. Předpokládá se, že napadl 300 000 počítačů.

Válka na Ukrajině – 2022

Od začátku války na Ukrajině vede Rusko hybridní válku. Šíří dezinformace o aktuálním děním a příčině války. Tato kampaň se projevuje i v zemích NATO a EU. Můžete na sociálních sítích narazit na články pomlouvající danou politickou osobnost či zpochybňující právo Ukrajiny na daná teritoria a další nesmysli, které znalci v oboru dokážou snadno vyvrátit. Je tedy faktem že tato kampaň se neštítí ničeho. Štve občany země proti sobě a cílí na chaos, který pomůže k moci těm stranám a osobám, které půjdou Ruské federaci takzvaně na ruku. Aktualitou

v tomto dění je využívání AI pro tvorbu falešných videí, fotografií, článků a ohýbání pravdy. Deepfake videa, jsou též aktuálním problémem. Tyto programy vytváří fiktivní videa známých osob říkající věci, které nikdy neřekli, dokonce s jejich vlastním hlasem.

CrowdStrike – 2024

Bezpečnostní firma Crowdstrike, která spolupracuje s Microsoftem a podílela se i na vyšetřování voleb v USA v roce 2016. Vydala v červenci aktualizaci, která zapříčinila výpadek 8,5 milionů Windows zařízení na celém světě. Jedná se tak pravděpodobně o jeden z největších výpadků a incidentů v historii. Výpadek způsobil vážné problémy mnohým firmám. A ukázal že i profesionální firma jako je Crowdstrike může udělat chybu. Nešťastným rozhodnutím bylo, že jako omluvu svým partnerům zvolili desetidolarové poukázky na kafe, které po krátkém čase přestali platit.

Seznam použitých zdrojů

Knižní zdroje:

1. VONDRUŠKA, Pavel. *Kryptologie, šifrování a tajná písma*. Klub mladých čtenářů. Praha: Albatros, 2006. ISBN 80-00-01888-8.
2. AUMASSON, Jean-Philippe. *Serious cryptography: a practical introduction to modern encryption*. San Francisco: No Starch Press, [2018]. ISBN 978-1-59327-826-7.
3. BURDA, Karel. *Aplikovaná kryptografie*. Brno: Vutium, 2013. ISBN 978-80-214-4612-0.
4. BURDA, Karel. *Úvod do kryptografie*. Brno: Akademické nakladatelství CERM, 2015. ISBN 978-80-7204-925-7.
5. BURDA, Karel. *Kryptografie okolo nás*. CZ.NIC. Praha: CZ.NIC, z.s. p.o., 2019. ISBN 978-80-88168-49-2.
6. PICKOVER, Clifford A. *Kniha o fyzice: od velkého třesku ke kvantovému znovuzrození: 250 milníků v dějinách fyziky*. Zip. Praha: Dokořán, 2015. ISBN 978-80-7363-609-8.
7. PICKOVER, Clifford A. *Matematická kniha: od Pythagora po 57. dimenzi : 250 milníků v dějinách matematiky*. Zip. Praha: Argo, 2012. ISBN 978-80-257-0705-0.

8. STROUKAL, Dominik. *Dark Web: sex, drogy a bitcoiny*. Praha: Grada, 2020. ISBN 9788027129348.
9. ANTAL, Eugen. ZAJAC, Antal. Cryptologia vol. 47 issue 3
10. SNOWDEN, Edward J. *Nesmazatelné záznamy*. Klokan. Frýdek-Místek: Alpress, 2020. ISBN 978-80-7633-216-4.
11. JIRÁSEK, Petr; NOVÁK, Luděk a POŽÁR, Josef. *Výkladový slovník kybernetické bezpečnosti*. Páté doplněné a upravené vydání. Praha: Česká pobočka AFCEA, 2022. ISBN 978-80-908388-4-0.
12. DIMAGGIO, Jon. *The art of cyberwarfare: an investigator's guide to espionage, ransomware, and organized cybercrime*. San Francisco: No Starch Press, [2022]. ISBN 978-1-7185-0214-7.

Webové zdroje:

1. Oficiální web standardů NIST. Online. Dostupné z: https://www.nist.gov. [cit. 2025-01-06].
2. Webové stránky muzea Kryptologie NSA. Online. Dostupné z:

https://www.nsa.gov/museum/. [cit. 2025-01-06].
3. Nizozemské online muzeum Kryptologie. Online. Dostupné z: https://www.cryptomuseum.com. [cit. 2025-01-06].
4. Computerphile. Online. Dostupné z: https://www.youtube.com/@Computerphile. [cit. 2025-01-06].
5. Cardonův šifrovací autoklíč. Online. Dostupné z: https://crypto.interactive-maths.com/autokey-cipher.html. [cit. 2025-01-06].
6. OTP – Claude Shannon. Online. Dostupné z: https://ieeexplore.ieee.org/document/6769090. [cit. 2025-01-06].
7. Téma D-Wave QA. Online. Dostupné z: https://qubits.cz/novinky/tydenni-prehled-39-2022-kvantovy-a-kvantove-inspirovany-annealing-zihani-pokroky-se-spinovymi-qubity-a-quantum-sdk-od-intelu/. [cit. 2025-01-06].
8. Téma D-Wave QA. Online. Dostupné z: https://qubits.cz/novinky/tydenni-prehled-39-2022-kvantovy-a-kvantove-inspirovany-annealing-zihani-pokroky-se-spinovymi-

qubity-a-quantum-sdk-od-intelu/. [cit. 2025-01-06].
9. Reakce IBM na NASA a Google. Online. Dostupné z: https://www.science.org/content/article/ibm-casts-doubt-googles-claims-quantum-supremacy. [cit. 2025-01-06].
10. Telegraf. Online. Dostupné z: https://www.pens.co.uk/pen2paper/wp-content/uploads/2014/08/A-History-of-Telegraphy.pdf. [cit. 2025-01-06].
11. Telegraf. Online. Dostupné z: https://www.history.com/topics/inventions/telegraph. [cit. 2025-01-06].
12. Telegraf. Online. Dostupné z: https://www.irozhlas.cz/veda-technologie/historie/telegraf-samuel-morse-komunikace-185-let_2209040702_fos. [cit. 2025-01-06].
13. Telefon. Online. Dostupné z: https://www.nationalitpa.com/history-of-telephone. [cit. 2025-01-06].
14. Telefon. Online. Dostupné z: https://www.history.com/topics/inventions/alexander-graham-bell. [cit. 2025-01-06].

15. Telefon. Online. Dostupné z: https://www.alza.cz/historie-mobilnich-telefonu. [cit. 2025-01-06].
16. 5G konspirační teorie. Online. Dostupné z: https://www.theguardian.com/technology/2019/jul/26/how-baseless-fears-over-5g-rollout-created-a-health-scare. [cit. 2025-01-06].
17. Wi-Fi historie. Online. Dostupné z: https://www.cablefree.net/history-of-wifi-technology/. [cit. 2025-01-06].
18. Computerworld. Online. Dostupné z: https://www.earchiv.cz/a95/a504c502.php3. [cit. 2025-01-06].
19. RFC-1118. Online. Dostupné z: https://datatracker.ietf.org/doc/html/rfc1118. [cit. 2025-01-06].
20. RFC-791. Online. Dostupné z: https://datatracker.ietf.org/doc/html/rfc791. [cit. 2025-01-06].
21. Historie WWW podle web foundation. Online. Dostupné z: https://webfoundation.org/about/vision/history-of-the-web/. [cit. 2025-01-06].
22. Vznik WWW v CERN. Online. Dostupné z: https://home.cern/science/computing/birth-web/short-history-web. [cit. 2025-01-06].

23. WWW standardy. Online. Dostupné z: https://www.w3.org/standards/. [cit. 2025-01-06].
24. Verze WWW. Online. Dostupné z: https://www.simplilearn.com/what-is-web-1-0-web-2-0-and-web-3-0-with-their-difference-article. [cit. 2025-01-06].
25. Historie CSS. Online. Dostupné z: https://www.geeksforgeeks.org/css-history-versions/. [cit. 2025-01-06].
26. Historie JS. Online. Dostupné z: https://www.w3schools.com/js/js_history.asp. [cit. 2025-01-06].
27. Omluva autora za chyby v JS. Online. Dostupné z: https://lunduke.substack.com/p/creator-of-javascript-apologizes. [cit. 2025-01-06].
28. Historie Googlu. Online. Dostupné z: https://about.google/our-story/. [cit. 2025-01-06].
29. Historie projektu Mozilla. Online. Dostupné z: https://www.mozilla.org/en-US/about/history/. [cit. 2025-01-06].
30. Internet explorer historie. Online. Dostupné z: https://www.microsoft.com/en-us/edge/learning-center/how-internet-

explorer-once-took-over-the-web?form=MA13I2. [cit. 2025-01-06].
31. Bezpečnostní riziko opera? Online. Dostupné z: https://www.sec.gov/ix?doc=/Archives/edgar/data/0001737450/000143774924012913/opra20231231_20f.htm. [cit. 2025-01-06].
32. TOR projekt. Online. Dostupné z: https://www.torproject.org/about/history/. [cit. 2025-01-06].
33. Historie Operačních systémů. Online. Dostupné z: https://www.youtube.com/watch?v=1lG7lFLXBIs. [cit. 2025-01-10].
34. Historie Linuxu. Online. Dostupné z: https://www.youtube.com/watch?v=ShcR4Zfc6Dw. [cit. 2025-01-10].
35. Historie Unixu. Online. Dostupné z: https://unix.org/what_is_unix/history_timeline.html. [cit. 2025-01-10].
36. Historie GUI. Online. Dostupné z: https://www.wired.com/1997/12/web-101-a-history-of-the-gui/. [cit. 2025-01-10].
37. Český článek o historii windows. Online. Dostupné z: https://www.novinky.cz/clanek/internet-a-pc-

software-windows-95-byly-ve-svete-pocitacu-revoluci-40334237. [cit. 2025-01-10].
38. Unixové války. Online. Dostupné z: https://www.bell-labs.com/unix-history/wars.html. [cit. 2025-01-10].
39. Unixové války jako válka o standardizaci. Online. Dostupné z: https://klarasystems.com/articles/unix-wars-the-battle-for-standards/. [cit. 2025-01-10].
40. BSD. Online. Dostupné z: https://docs.freebsd.org/en/articles/explaining-bsd/. [cit. 2025-01-10].
41. Historie Androidu. Online. Dostupné z: https://www.androidauthority.com/history-android-os-name-789433/. [cit. 2025-01-10].
42. Časová linka programovací. Online. Dostupné z: https://www.computer.org/publications/tech-news/insider-membership-news/timeline-of-programming-languages. [cit. 2025-01-10].
43. Tutoriál na programování v Assembly. Online. Dostupné z: https://www.tutorialspoint.com/assembly_programming/index.htm. [cit. 2025-01-10].

44. Fortran. Online. Dostupné z: https://fortran-lang.org/. [cit. 2025-01-10].
45. Historie Fortranu. Online. Dostupné z: https://www.ibm.com/history/fortran. [cit. 2025-01-10].
46. Cobol. Online. Dostupné z: https://www.root.cz/clanky/programovani-mainframu-cobol/. [cit. 2025-01-10].
47. Historie Basicu. Online. Dostupné z: https://www.thoughtco.com/history-basic-programming-language-1991662. [cit. 2025-01-10].
48. Historie jazyku Pascal. Online. Dostupné z: https://www.revelo.com/blog/pascal-programming-language. [cit. 2025-01-10].
49. Vývoj jazyka C. Online. Dostupné z: https://www.bell-labs.com/usr/dmr/www/chist.html. [cit. 2025-01-10].
50. SQL. Online. Dostupné z: https://www.ibm.com/think/topics/structured-query-language. [cit. 2025-01-10].
51. Programovací jazyk Karel. Online. Dostupné z: https://web.stanford.edu/class/cs106j/lectures/02-Programming-In-Karel/02-Programming-In-Karel.pdf. [cit. 2025-01-10].

52. C++. Online. Dostupné z: https://www.oreilly.com/library/view/object-oriented-programming/9789332503663/xhtml/head-0045.xhtml. [cit. 2025-01-10].
53. Krátká historie C++. Online. Dostupné z: https://www.perforce.com/blog/qac/misra-cpp-history. [cit. 2025-01-10].
54. Perl. Online. Dostupné z: https://www.perl.org/about.html. [cit. 2025-01-10].
55. Vývoj perlu. Online. Dostupné z: https://www.techopedia.com/2/29271/development/programming-languages/perl-101. [cit. 2025-01-10].
56. O Pythonu. Online. Dostupné z: https://pythoninstitute.org/about-python. [cit. 2025-01-10].
57. O Ruby. Online. Dostupné z: https://www.ruby-lang.org/en/about/. [cit. 2025-01-10].
58. Historie Java. Online. Dostupné z: https://www.javatpoint.com/history-of-java. [cit. 2025-01-10].
59. Historie PHP. Online. Dostupné z: https://www.php.net/manual/en/history.php.php. [cit. 2025-01-10].

60. Historie jazyka C. Online. Dostupné z: https://historytimelines.co/timeline/c. [cit. 2025-01-10].
61. C# dokumentace. Online. Dostupné z: https://learn.microsoft.com/en-us/dotnet/csharp/whats-new/csharp-version-history. [cit. 2025-01-10].
62. C# dokumentace. Online. Dostupné z: https://go.dev/talks/2012/splash.article. [cit. 2025-01-10].
63. Článek o Swiftu. Online. Dostupné z: https://www.progkids.com/en/blog/swift. [cit. 2025-01-10].
64. *Deklerace nezávislosti internetu*. Online. Dostupné z: https://www.eff.org/cyberspace-independence. [cit. 2025-02-12].
65. *John Perry Barlow*. Online. Dostupné z: https://www.eff.org/john-perry-barlow. [cit. 2025-02-12].
66. *DEF CON. Online*. Dostupné z: https://defcon.org/html/links/dc-about.html. [cit. 2025-02-12].
67. *Chaos Computer Club část 1*. Online. Dostupné z:

https://www.nycresistor.com/2008/06/28/the-chaos-computer-club-1981-1984/. [cit. 2025-02-16].
68. *Chaos Computer Club část 2*. Online. Dostupné z: https://www.nycresistor.com/2008/07/04/cats-dataloos-and-a-btx-bank-robbery/. [cit. 2025-02-16].
69. *Wired o CCC.* Online. Dostupné z: https://www.wired.com/2008/07/the-history-of-3/. [cit. 2025-02-16].
70. *Archív webu cDc*. Online. Dostupné z: https://web.archive.org/web/20150506102919/https://w3.cultdeadcow.com/cms/team_bio.html. [cit. 2025-02-17].
71. *Článek o cDc*. Online. Dostupné z: https://cyber.tap.purdue.edu/blog/articles/hacktivism-the-cult-of-the-dead-cow/. [cit. 2025-02-17].
72. *4chan*. Online. Dostupné z: https://www.uva.nl/en/shared-content/faculteiten/en/faculteit-der-geesteswetenschappen/news/2024/06/4chan-from-anarchic-internet-forum-to-

breeding-ground-for-the-far-right.html. [cit. 2025-02-17].
73. *Pirates Bay*. Online. Dostupné z: https://techbullion.com/the-history-of-pirate-bay-everything-you-need-to-know/. [cit. 2025-02-22].
74. *Kevin Mitnick*. Online. Dostupné z: https://www.mitnicksecurity.com/about-kevin-mitnick-mitnick-security. [cit. 2025-02-22].
75. *CryptoLocker*. Online. Dostupné z: https://www.proofpoint.com/us/threat-reference/cryptolocker. [cit. 2025-02-22].
76. *WikiLeaks.* Online. Dostupné z: https://wikileaks.org/What-is-WikiLeaks.html. [cit. 2025-02-22].
77. *Český článek o LulzSec*. Online. Dostupné z: https://zing.cz/article/historie-lulzsec-den-po-dni. [cit. 2025-02-22].
78. *The Guardian článek o LulzSec*. Online. Dostupné z: https://www.theguardian.com/technology/2013/may/16/lulzsec-hacking-fbi-jail. [cit. 2025-02-22].

79. *Článek o Silk Road.* Online. Dostupné z: https://www.investopedia.com/terms/s/silk-road.asp. [cit. 2025-02-22].
80. *Ross W. Ulbricht.* Online. Dostupné z: https://www.theguardian.com/technology/2013/oct/03/five-stupid-things-dread-pirate-roberts-did-to-get-arrested. [cit. 2025-02-22].
81. *Zásahy do ukrajinských voleb 2014*. Online. Dostupné z: https://cyberlaw.ccdcoe.org/wiki/Ukrainian_parliamentary_election_interference_(2014). [cit. 2025-02-22].
82. *Časová osa GDPR.* Online. Dostupné z: https://www.edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en. [cit. 2025-02-22].
83. *Shrnutí GDPR*. Online. Dostupné z: https://www.gdprsummary.com/gdpr-summary/. [cit. 2025-02-22].
84. Volby USA 2016. Online. Dostupné z: https://edition.cnn.com/2016/12/26/us/20

16-presidential-campaign-hacking-fast-facts/index.html. [cit. 2025-02-22].
85. *WannaCry.* Online. Dostupné z: https://www.fortinet.com/resources/cyberglossary/wannacry-ransomware-attack. [cit. 2025-02-22].
86. *Boj EU s ruskými dezinformacemi.* Online. Dostupné z: https://www.consilium.europa.eu/en/documents-publications/library/library-blog/posts/the-fight-against-pro-kremlin-disinformation/. [cit. 2025-02-22].
87. *Crowdstrike poukázky.* Online. Dostupné z: https://www.novinky.cz/clanek/ekonomika-crowdstrike-se-svym-partnerum-omluvil-za-it-vypadek-poukazem-na-10-dolaru-sklidil-posmech-40481721. [cit. 2025-02-22].