



Kapitola [Internet věcí]

Projekt: B-SAFE

Číslo: 2018-1CZ01-KA204-048148

Jméno autora: EDIT VALUE®

Poslední zpracování: 02.09.2020

Internet věcí

Úvod

Internet věcí, obecně známý jako IoT (Internet of Things), je součástí čtvrté průmyslové revoluce neboli Průmyslu 4.0 a má přímý dopad na jednotlivce jako koncového uživatele.



IoT je systém vzájemně propojených výpočetních zařízení, mechanických a digitálních strojů, objektů, zvířat nebo osob, který je schopen přenášet data po síti, aniž by vyžadoval interakci mezi dvěma lidmi nebo mezi člověkem a počítačem. Prvním „oficiálním“ IoT zařízením byl automat na kolu v kampusu na Carnegie-Mellonově univerzitě v Pittsburghu, Pensylvánii, v roce 1982. Studenti chtěli mít možnost dopředu zjistit, zda jsou nově naložené plechovky limonády dostatečně vychlazené, a proto stroj upravili tak, aby tuto informaci hlásil počítači v nedaleké kanceláři.

Navzdory svému věku se IoT technologie neustále vyvíjejí a přinášejí do našich každodenních životů změny, kterým musíme neustále čelit, neboť existuje bezpočet příležitostí a nových možných způsobů využití IoT ať už v průmyslovém prostředí, nebo v každodenním životě.

Přestože tyto technologie poskytují účinná a efektivní řešení mnoha problémů reálného světa, pojí se s nimi významné výzvy týkající se bezpečnosti a soukromí, které nesmíme ignorovat.

Praktický význam – K čemu získané znalosti a dovednosti využijete

Nastudováním této kapitoly získáte znalosti o tom, co je to internet věcí a jaké existují hlavní způsoby využití této nové technologie.

Dále se dozvíte o nejběžnějších problémech souvisejících s bezpečností a ochranou soukromí při užívání IoT a o tom, jak reagovat v případě kybernetického útoku na Vaše chytré zařízení.

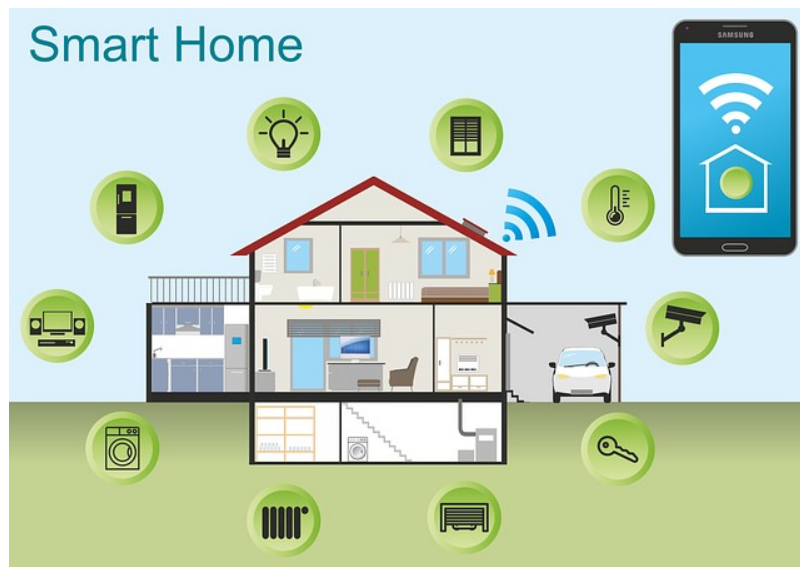
1. Internet věcí a jeho využití v každodenním životě

V průběhu let došlo k rychlému růstu v oblasti internetu věcí (IoT) jak z hlediska vývoje technologií, tak i tržního růstu. Síť počítačů nazvaná „Internet“ způsobila revoluci ve způsobu, jakým sdílíme informace. Internet věcí lze považovat za další revoluci v tom, jak vnímáme a sdílíme informace (Virat, 2018). Níže v rámečku máte uvedenou zjednodušenou definici internetu věcí:

Definice

Koncept **internetu věcí** umožňuje připojení jakéhokoliv zařízení (pokud má ON-OFF vypínač) k internetu nebo k jiným zařízením. IoT je obrovská síť propojených zařízení a lidí, kteří shromažďují a sdílí data o způsobu jejich použití a o prostředí kolem nich.

Zařízení a předměty se zabudovanými senzory jsou připojeny k IoT platformě, která integruje data z různých zařízení a používá analýzy ke sdílení nejcennějších informací s aplikacemi vytvořenými pro řešení specifických potřeb. Na obrázku níže vidíte dva příklady IoT technologie:



Jak jste se již dozvěděli, internet věcí je široký pojem používaný k označení rozsáhlé sítě zařízení připojených k internetu.

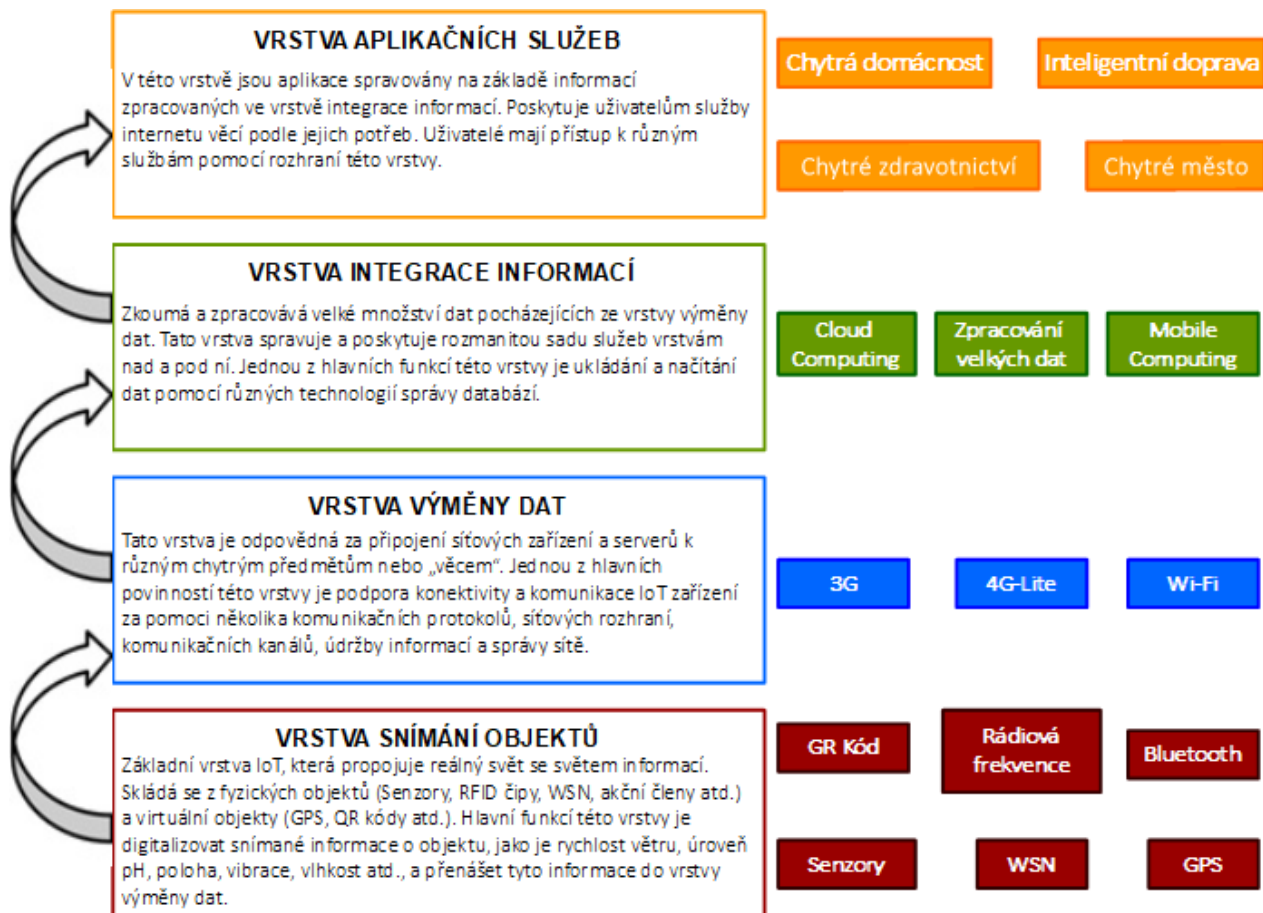


Internet věcí se zavazuje, že bude pro spotřebitele nejvýznamnějším technologickým pokrokem od nástupu chytrých telefonů. Odborníci se domnívají, že tato technologie přinese do roku 2021 roční příjmy přesahující 123 miliard dolarů. Dále statistiky poukazují na to, že do konce roku 2020 bude k internetu připojeno více než 36 miliard zařízení.

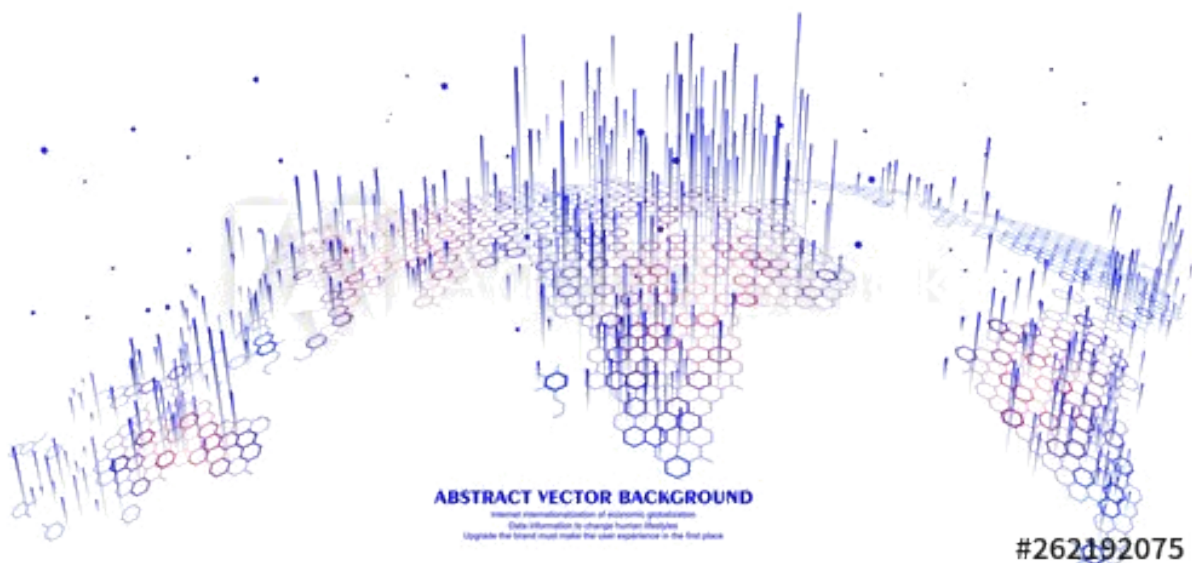
Velké společnosti, jako jsou Amazon, Google a Tesla, již v současné době spolupracují se službami v oblasti vývoje softwaru na výrobě špičkových IoT zařízení. Předpokládá se, že díky IoT technologiím se stanou vyspělé chytré domácnosti realitou. Mezi další příklady IoT technologií patří **autonomní vozidla, nositelná zařízení, která monitorují zdraví nebo změny v chování pacientů, hlasoví asistenti (například Alexa), systém chytrého vytápění atd.**

Díky tomu lze předpokládat, že dospějeme do okamžiku, kdy bude celá společnost používat IoT zařízení. Proto je velmi důležité poučit lidi o internetu věcí, a především o tom, jak si s jeho **zavedením zachovat soukromí a bezpečnost.**

Dynamika, inteligence a mobilita internetu věcí z něj činí vysoce poptávanou technologii, ale také jej dělá **zranitelným a rizikovým z hlediska bezpečnosti a ochrany soukromí.** Abyste pochopili složitost tohoto problému, musíte nejprve pochopit základní architekturu internetu věcí, která se vyznačuje **dynamickou strukturou.** Počet vrstev, které tvoří architekturu IoT, se mezi odborníky značně liší, ale všichni se shodují na tom, že se IoT skládá nejméně z těchto čtyř vrstev: **vrstva snímání objektů, vrstva výměny dat, vrstva integrace informací a vrstva aplikačních služeb.**



Jak si můžete všimnout, vrstva aplikačních služeb usnadňuje celosvětovou správu chytrých aplikací a poskytuje uživateli konkrétní služby. V následující tabulce jsou uvedeny hlavní způsoby využití IoT v



každodenním životě:

Chytrá

Jedná se o propojený domov, ve kterém všechny druhy elektroniky vzájemně



domácnost	spolupracují prostřednictvím internetu. Například Vám chytrá domácnost umožňuje cestou z práce zapnout klimatizaci nebo pračku. Stručněji řečeno, vše je propojeno za účelem udělat Váš život jednodušší a pohodlnější.
Nositelná elektronika	Tato zařízení (například Fit Bit) shromažďují data a informace o uživateli, které jsou později zpracovány tak, aby se z nich získaly důležité poznatky. Tyto malé, vysoce výkonné přístroje široce pokrývají požadavky ohledně fitness, zdraví a zábavy.
Chytrá auta	Chytré vozidlo, které je schopno optimalizovat svůj vlastní provoz, údržbu i pohodlí cestujících. Tato vozidla se používají v inteligentní dopravě, která zahrnuje vodní cesty, železnice, silnice atd., a v reálném čase dostávají informace o silnicích, nehodách, odklonech a uzavírkách silnic takovým způsobem, který zajišťuje maximální bezpečnost pro řidiče a spolujezdce.
Chytrá města	Zahrnují vše, co tvoří město, jako je dohled, doprava, systémy hospodaření s energií, distribuce vody, městská bezpečnost a monitorování životního prostředí. Vláda může být například automaticky informována o naměřených úrovních znečištění nebo nedostatku dodávek energie atd.
Chytré zemědělství	Zemědělci využívají užitečné poznatky z dostupných dat, aby zajistili lepší návratnost investic. Některými z jednoduchých způsobů využití IoT jsou například snímání vlhkosti a živin v půdě, řízení spotřeby vody pro růst rostlin a určení vlastního hnojiva.
Inteligentní řízení spotřeby energie	Elektrizační sítě budoucnosti budou nejen dostatečně chytré, ale také vysoce spolehlivé. Využití inteligentních měřičů, domácích centrálních bran, inteligentních zásuvek a připojených spotřebičů pomáhá šetřit zdroje a peníze spotřebitelům, výrobcům i poskytovatelům služeb.
Chytré zdravotnictví	Propojený systém zdravotní péče a inteligentní lékařské přístroje představují revoluci pro společnost, neboť mají významný dopad nejen na firmy, ale i na celkové blaho lidí. Uplatňování IoT v oblasti zdravotnictví zahrnuje získávání informací o zdravotním stavu jedince, jako je krevní tlak, tělesná teplota, měření srdečního tepu atd., prostřednictvím malých, nízkoenergetických a vysoce účinných nositelných zařízení. Tyto shromážděné informace mohou být sdíleny s příslušnými jednotlivci a zdravotnickými středisky pro budoucí lékařské postupy.

1.Procvičte si znalosti

Cvičení /JEDNA MOŽNOST/

Související dílčí výukový cíl: DVC_Internet věcí_01_01: Dozvíte se o struktuře IoT a jak funguje.

Zadání: Co je to internet věcí?

Úkol: Vyberte správné odpovědi: pouze jedna odpověď je správná.

- Internet věcí je síť propojených serverů, které jsou dostupné prostřednictvím internetu.
- Internet věcí je digitalizace a automatizace všech částí společnosti i výrobních procesů.
- Internet věcí je globální síť, která navzájem propojuje počítače po celém světě.
- Internet věcí je začínající technologie, která se zaměřuje na propojení věcí nebo zařízení navzájem mezi sebou a mezi lidmi nebo uživateli za účelem dosažení některých společných cílů.

Cvičení /VÍCE MOŽNOSTÍ/

Související dílčí výukový cíl: DVC_Internet věcí_01_02: Dozvíte se, jaké existují IoT aplikace.



Zadání: Jaké jsou hlavní způsoby využití internetu věcí?

Úkol: Vyberte správné odpovědi: žádná, jedna, jedna a více nebo všechny odpovědi mohou být správně.

- Monitorování elektrického vedení a inteligentní elektrizační soustavy.
- Řízení dodavatelského řetězce v maloobchodě.
- Řízení dodavatelského řetězce v měnícím se průmyslu.
- Regulace vody v zemědělství.

2. Internet věcí a otázky ochrany soukromí a bezpečí

Inteligentní zařízení připojená k internetu věcí neustále shromažďují osobní informace o spotřebitelích. Proto jedna z největších obav souvisejících se zaváděním internetu věcí do našeho každodenního života souvisí se soukromím a bezpečností osobních či citlivých informací, neboť krádež osobních informací může způsobit vážnou újmu jednotlivcům, podnikům i celé společnosti. **IoT je všudypřítomná technologie** se složitou architekturou a strukturou. V důsledku toho vytváří **nové problémy v oblasti bezpečnosti a ochrany soukromí**, které byly dosud považovány za neškodné nebo nespecifikované. Tyto obavy se týkají především:

1. **IoT technologie mají** ve srovnání s chytrými telefony nebo stolními počítači **delší životnost**.
2. Existuje **celá řada výrobců**, většina z nich postrádá tradiční odborné znalosti v oblasti informačních technologií (IT), což má za následek problémy s interoperabilitou a špatnou bezpečnostní hygienu.
3. Tento **nedostatek odborných znalostí v oblasti IT** se rozšíří i na koncové uživatele (kteří jsou de facto správci systému).
4. Počet zařízení a globální propojenost obecně všechny problémy zhoršují. Odhaduje se, že v současné době je připojeno 50 miliard zařízení.

Bezpečnost dat a soukromí uživatelů jsou odlišné pojmy, vzájemně se však nevylučují. Bezpečnostní útok nebo kybernetický útok totiž automaticky narušuje i soukromí uživatele.

Výzvy, které je třeba překonat, aby bylo možné vyřešit problémy spojené s bezpečností a ochranou soukromí v oblasti internetu věcí, jsou obrovské. Důvodem je především mnoho omezení spojených s poskytováním bezpečnosti a soukromí v IoT systémech. Níže v rámečku je uvedena stručná definice pojmů, které se na internet věcí vztahují.

Druhy hrozeb a útoků na bezpečnost a soukromí, kterým je IoT vystavován, závisí na jeho vrstvách, protože každá vrstva má odlišné zvláštnosti a související technologie. V následující tabulce je zobrazen souhrn nejběžnějších kybernetických útoků na IoT a stupeň dopadu na čtyři vrstvy, které tvoří architekturu IoT:

Stručný popis		VRSTVA SNÍMÁNÍ OBJEKTŮ	VRSTVA VÝMĚNY DAT	VRSTVA INTEGRACE INFORMACÍ	VRSTVA APLIKAČNÍCH SLUŽEB
Škodlivý kód	Jakýkoli kód v kterékoli části softwarového systému nebo skriptu, který má za úkol způsobit nežádoucí následky, narušit bezpečnost nebo poškodit systém.	Vysoká	Vysoká	Nízká	Vysoká
DoS útok	Kybernetický útok, při kterém se pachatel snaží znepřístupnit stroj nebo	Nízká	Vysoká	Vysoká	Nízká



Směrovací protokol	síťový prostředek Protokoly, které mohou směrovače používat k výměně informací o topologii sítě	Nízká	Vysoká	Vysoká	Nízká
Odposlouchávání	Je tajné nebo kradmé naslouchání soukromé konverzaci nebo komunikaci druhých bez jejich souhlasu	Vysoká	Střední	Vysoká	Střední
Krádež identity	Záměrné použití identity někoho jiného, obvykle jako způsob k získání finanční výhody nebo jiných osobních informací	Vysoká	Střední	Vysoká	Střední
Sinkhole útok	Ohrožuje zabezpečení WSN (Wireless Sensor Network) téměř v každé vrstvě jejího protokolu	Střední	Vysoká	Nízká	Nízká
Phishingový útok	Podvodný pokus o získání citlivých informací nebo údajů obvykle prováděný pomocí falšování e-mailových adres odesílatele (spoofing) nebo zaslání okamžitých zpráv	Nízká	Nízká	Střední	Vysoká



Jak vidíte, existuje celá řada možných útoků, které mohou ohrozit bezpečnost a soukromí IoT zařízení s různou úrovní dopadu v závislosti na vrstvě. Všechny zúčastněné strany, výrobce nebo vývojář, vláda a koncový uživatel, tedy musí řešit značné výzvy spojené s užíváním internetu věcí.

2.Procvičte si znalosti

Cvičení /VÍCE MOŽNOSTÍ/



Související dílčí výukový cíl: DVC_Internet věcí_02_01: Dozvíte se o bezpečnostních problémech spojených s IoT.

Zadání: Která z následujících tvrzení týkajících se zabezpečení IoT zařízení jsou pravdivá?

Úkol: Vyberte správné odpovědi: žádná, jedna, jedna a více nebo všechny odpovědi mohou být správně.

- Při generování a ukládání dat je vyžadováno zabezpečení dat.
- Bezpečnostní požadavky na aplikace IoT musí být aplikovány ve třech vrstvách: vrstva aplikačních služeb, vrstva výměny dat a vrstva snímání objektů.
- Pravděpodobnost výskytu phishingového útoku v IoT zařízení je vyšší ve vrstvě integrace informací.
- Architektura IoT umožňuje škůdcům využít zranitelná místa, která jsou charakteristická pro každou z vrstev internetu věcí.
- Škodlivý kód může mít vliv na nejméně tři vrstvy.

Cvičení /JEDNA MOŽNOST/

Související dílčí výukový cíl: DVC_Internet věcí_02_02: Dozvíte se o problémech ochrany soukromí spojených s IoT.

Zadání: Které z následujících tvrzení týkající se ochrany soukromí při užívání IoT zařízení je pravdivé?

Úkol: Vyberte správné odpovědi: pouze jedna odpověď je správná.

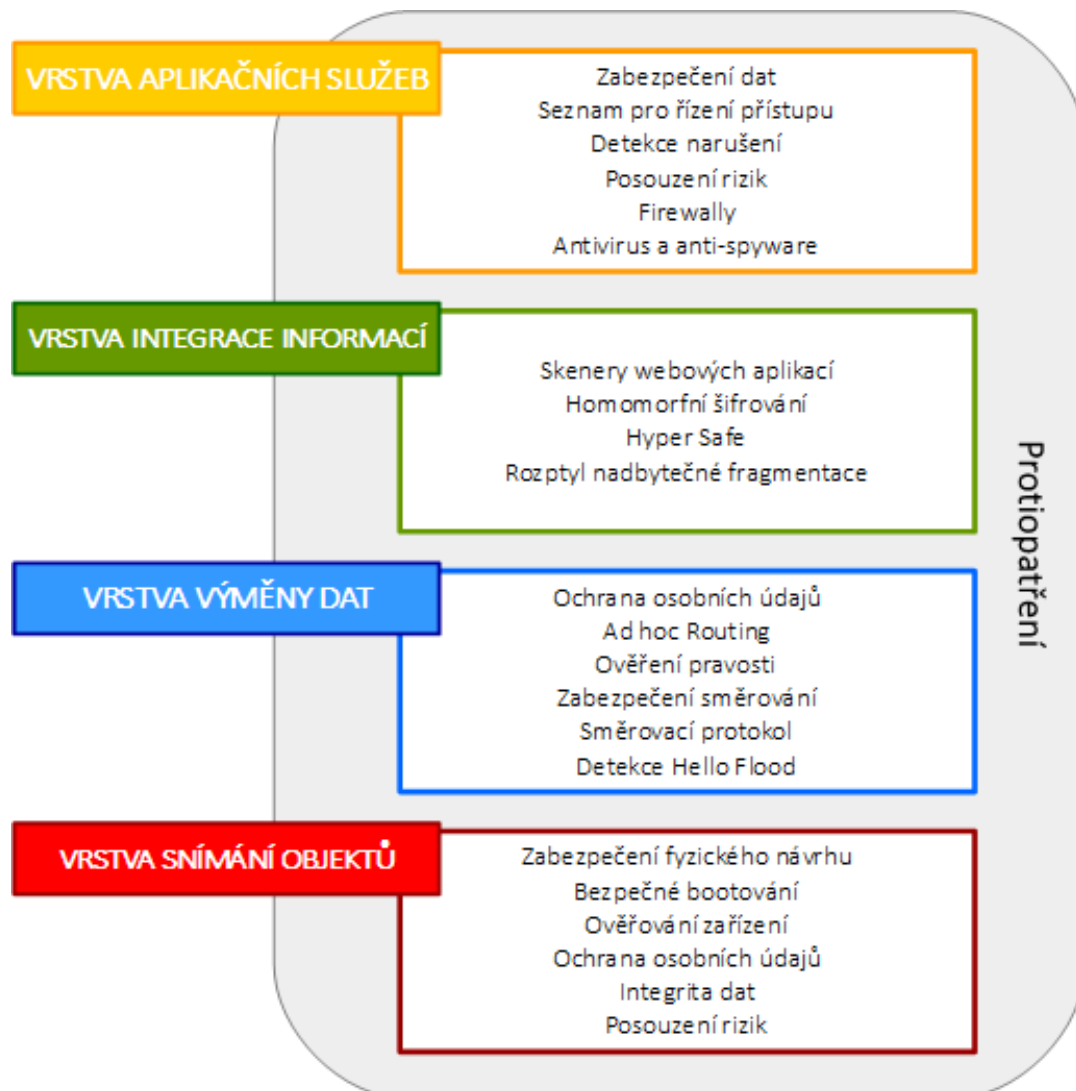
- Významný nárůst užití IoT v posledních letech s sebou přinesl několik otázek ohledně bezpečnosti, protože kromě společných a obvyklých vlastností IoT ji ohrožuje snižující se dostupnost dat.
- Výrobci musí zaručit ochranu osobních údajů uživatelů, které souvisejí s jejich aktivitami, návyky a interakcemi.
- Soukromí se v tomto případě týká toho, jak dobře se dokážou IoT zařízení bránit před odcizením uživatelských dat.
- Soukromí je ohrožováno pouze ve vrstvě aplikačních služeb.

3. Internet věcí a ochrana uživatelů

Na začátku roku 2019 se CNN podařilo získat přístup k živým přenosům z různých kamer pomocí vyhledávače pro zařízení IoT Shodan. Na dálku sledovali děti, jak si hrají v tělocvičně střední školy v Indonésii, muže chystajícího se do postele v moskevském bytě, australskou rodinu přicházející a odcházející z jejich garáže a ženu krmící kočku v Japonsku. Zdálo se, že si nikdo z nich neuvědomuje, že každá sekunda jejich života je vysílána na internetu. Podle CNN žádná z kamer neprošla bezpečnostní kontrolou a byla přístupná každému, kdo znal správnou adresu.



Abyste se nedostali do podobné situace, existují určité **metody, postupy a způsoby chování**, které by měl **přijmout jak vývojář IoT zařízení, tak Vy jako koncový uživatel**. Níže můžete vidět některá opatření prevence a reakce na kybernetické útoky ve všech vrstvách IoT zařízení.



Jak můžete vidět, většina mechanismů ochrany soukromí a zabezpečení pro IoT by měla být implementována. Vývojáři IoT by se měli zaměřit na **tvorbu zařízení, která jsou fyzicky zabezpečena** a chráněna kryptografickými algoritmy, platformami se zesílenou vstupní bránou, komplexním šifrováním, antivirem, anti-spywarem, anti-adwarem a dalšími pokročilými a pravidelně aktualizovanými bezpečnostními technikami. Uživatel by se tak mohl spolehnout na bezpečnostní mechanismus, který je již zabudovaný v IoT zařízení a který má zajistit jeho bezpečí a ochranu soukromí. Přesto existují některé kroky, kterých si jako spotřebitel IoT musíte být vědomi, abyste překonali různá nebezpečí, která hrozí zabezpečení a ochraně osobních údajů:

1. – Přečtěte si bezpečnostní požadavky a zásady ochrany osobních údajů zařízení

Vždy si vyberte zařízení IoT od důvěryhodného a transparentního výrobce. Máte právo být obeznámeni s bezpečnostní technikou zahrnutou v IoT.



Také byste si měli vždy **přečíst zásady ochrany osobních údajů** zařízení, abyste věděli, jak Vaše zařízení IoT funguje, a proč jsou Vaše data shromažďována a používána inteligentními zařízeními IoT. Jednoduše řečeno, před použitím zařízení IoT byste měli vědět:

- 1) Zda máte možnost dostat se k Vaším datům, zobrazit je a smazat;
- 2) Zda můžete odpojit Vaše IoT zařízení, kdykoliv chcete;
- 3) Zda máte možnost dát souhlas ke shromažďování Vašich osobních údajů na IoT zařízení.

2. – Přestaňte používat výchozí heslo!

První, co byste na svém zařízení IoT měli zkontrolovat je, zda máte možnost **změnit výchozí heslo**. Vždy používejte silná a unikátní hesla pro každé zařízení, které vlastníte. Nezapomeňte si také změnit heslo svého Wi-Fi routeru!

3. – Deaktivujte vzdálený přístup (WAN – Wide Area Network) k zařízení

Pokud se právě nacházíte doma, vygooglujte si na svém počítači „jaká je moje IP adresa“. To, co se před Vámi objeví, je Vaše WAN IP adresa. Tato adresa je na internetu v jakémkoliv okamžiku jedinečná. Pokud někam vycestujete, tato IP adresa Vám umožní vzdálený přístup k Vaším chytrým domácím zařízením. Pokud zařízení nejsou zabezpečena, IP adresa je to jediné, co útočníci potřebují, aby k nim získali přístup. Tímto způsobem dokázalo CNN získat přístup k různým kamerám ve výše zmíněném příkladu!

4. – Vypněte si funkce, které nepoužíváte

Spolehlivé chytré zařízení je takové zařízení, které Vám umožňuje **přizpůsobit si jeho funkce**. Pokud například nepoužíváte své chytré hodinky ke shromažďování nejnovějších dat o Vašem cvičení, vypněte Bluetooth připojení, nebo pokud nepotřebujete zaznamenávat svou trasu běhu, vypněte GPS a sledování polohy.

5. – Staňte se přeborníkem v kybernetické bezpečnosti!

Věděli jste, že 95 % případů narušení kybernetické bezpečnosti je zapříčiněno lidskou chybou? Proto je **gramotnost v oblasti kybernetické bezpečnosti** nejdůležitější prevencí kybernetických útoků. Abyste se stali agentem 007 kybernetické bezpečnosti, musíte zvládnout všechny fáze plánu **šíření povědomí v oblasti kybernetické bezpečnosti**:



Ať už používáte zařízení IoT ve svém každodenním životě, jste majitelem podniku nebo manažer, který používá technologie a internet při každodenních činnostech, musíte **zvýšit své šance na zachycení útoku na Vaše bezpečí či soukromí předtím, než se plně odehraje**, minimalizovat škody a snížit náklady na obnovu dat.



Nyní máte všechny základní znalosti, které potřebujete k identifikaci hrozeb a zranitelných míst, k zhodnocení rizik a ochraně zařízení. Ale co když se i přes veškerou prevenci a opatrnost při používání internetu věcí stanete obětí kybernetického útoku? Odpověď na tuto otázku se opírá o tyto **4 body: Kdo, Co, Kdy a Jaké**.

KDO

Připravte si seznam osob, kterým můžete v případě nějakého incidentu zavolat. Je důležité, abyste věděli, kdo rozhodne o zahájení procesu obnovy a kdo bude hlavním spojením mezi Vámi a příslušnými pracovníky donucovacích orgánů.

CO

Ujistěte se, že máte vypracovaný plán ohledně toho, co dělat se svými daty v případě incidentu. To může zahrnovat vypnutí a restartování celých IoT systémů.

KDY

Určete, kdy upozornit krizový personál, odborníky na kybernetickou bezpečnost, poskytovatele služeb nebo pojišťovnu.

JAKÉ

Váš reakční plán by měl objasnit, jaké druhy činností představují hrozbu pro bezpečnost informací. Pokud se jedná o organizaci, jde o incidenty, jako je nefunkčnost webových stránek po delší než stanovenou dobu nebo důkaz o krádeži informací.

Nezapomeňte zapojit svou rodinu, přátele a/nebo zaměstnance do plánu šíření povědomí v oblasti kybernetické bezpečnosti, protože **každý uživatel internetu věcí je zodpovědný za její udržování!**

3. Procvičte si znalosti

Cvičení /VÍCE MOŽNOSTÍ/

Související dílčí výukový cíl: DVC_Internet věcí_03_01: Dozvíte se, jaká existují doporučení ochrany soukromí a bezpečí související s IoT.

Zadání: Jaká bezpečnostní opatření byste měli zavést, abyste zabránili kybernetickým útokům na svá IoT zařízení?

Úkol: Vyberte správné odpovědi: žádná, jedna, jedna a více nebo všechny odpovědi mohou být správně.

- a) Nainstalujte homomorfní šifrování.
- b) Nainstalujte firewall.
- c) Vytvořte rozptýl nadměrné fragmentace.
- d) Změňte výchozí heslo routeru.
- e) Vypněte na svých chytrých zařízeních funkce, které nepoužíváte.
- f) Deaktivujte vzdálený přístup k Vašemu zařízení.

Cvičení /VÍCE MOŽNOSTÍ/

Související dílčí výukový cíl: DVC_Internet věcí_03_02: Dozvíte se, jak se zachovat, pokud dojde k nějakému kybernetickému incidentu, který ohrožuje Vaše bezpečí.

Zadání: Co dělat, aby se z Vás stal agent 007 kybernetické bezpečnosti?



Úkol: Vyberte správné odpovědi: žádná, jedna, jedna a více nebo všechny odpovědi mohou být správně.

- g) Naučte se programovat, abyste dokázali šifrovat IoT zařízení.
- h) Vypracujte si pohotovostní plán založený na těchto 4 bodech: „Co je generováno?“, „Kde jsou data uložena?“, „Kdy se údaje používají?“ S kým jsou data sdílena?“.
- i) Vypracujte si pohotovostní plán založený na těchto 4 bodech: „Komu zavolat?“, „Jaký bude můj postup?“, „Kdy zalarmovat ostatní?“ a „Které činnosti lze považovat za incidenty?“.
- j) Zapojte celou svou rodinu, kolegy a zaměstnance do povědomí o kybernetické bezpečnosti.
- k) Vypracujte reakční plán až poté, co k nějakému incidentu dojde. Pouze takto jste schopni správně naplánovat, jak v budoucnosti postupovat.

Zdroje

Analytics Vidhya (August 26, 2016). *10 Real World Applications of Internet of Things (IoT) – Explained in Videos*. Retrieved from <https://www.analyticsvidhya.com/blog/2016/08/10-youtube-videos-explaining-the-real-world-applications-of-internet-of-things-iot/>

Clark, J. (November 17, 2016). *What is the Internet of Things (IoT)?* Retrieved from <https://www.ibm.com/blogs/internet-of-things/what-is-the-iot/>

Evans, D. (2011). *The internet of things how the next evolution of the internet is changing everything*. Cisco White Paper, 1–11. Retrieved from

https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

Griffiths, J. (February 2, 2019). *'Internet of things' or 'vulnerability of everything'? Japan will hack its own citizens to find out*. Retrieved from <https://edition.cnn.com/2019/02/01/asia/japan-hacking-cybersecurity-iot-intl>

Kelbert, J. (September 24, 2019). *5 Interesting Facts About the IoT*. Retrieved from <https://blog.flexis.com/5-interesting-facts-about-the-internet-of-things-iot>

Mena, D. M., Papapanagiotou, I. and Yang, B. (2018) *Internet of things: Survey on security*. Information Security Journal: A Global Perspective, 27:3, 162-182, DOI: 10.1080/19393555.2018.1458258

Finance Monthly (September 5, 2019). *The Worst And Weirdest IoT Hacks Of All Times*. Retrieved from <https://www.finance-monthly.com/2019/09/the-worst-and-weirdest-iot-hacks-of-all-times/>

Ngo, D. (December 22, 2015). *Home networking explained, part 9: Access your home computer remotely*. Retrieved from <https://www.cnet.com/how-to/home-networking-explained-part-9-access-your-home-computer-remotely/>

Oorschot, P. C and Smoth, S. W. (2019). *The Internet of Things: Security Challenges*. IEEE Security and Privacy Magazine, 17(5):7-9. DOI: 10.1109/MSEC.2019.2925918

Spencer, T. (August 8, 2019). *How to Respond to a Cyber Attack*. Retrieved from <https://www.industryweek.com/sponsored/article/22028042/how-to-respond-to-a-cyber-attack>

Viriati, M. S. et al. (2018). *Security and Privacy Challenges in Internet of Things*. Proceedings of the 2nd International Conference on Trends in Electronics and Informatics. IEEE Conference Record: # 42666; IEEE Xplore ISBN:978-1-5386-3570-4

Obrázky



<https://innovationatwork.ieee.org/low-power-low-latency-healthcare-iot/>
<https://messinaconstruction.com/smart-homes/smart-home-technology>

Zapamatujte si

Shrnutí

Internet věcí, zkráceně IoT, je v dnešní době populární výraz. IoT nepochybně změní způsob, jakým jednotlivci komunikují se světem a technologiemi kolem sebe a jeho síť **zařízení připojených k internetu** bude mít mnoho pozitivních dopadů.

IoT představuje revoluci ve způsobu komunikace a spolupráce mezi lidmi. Ve skutečnosti stojí IoT za celou řadou nových druhů interakce, jelikož je to **technologie, která nám pomocí internetu umožňuje propojení mezi věcmi, procesy, lidmi, zvířaty a téměř vším, co kolem sebe vidíme.**

Přestože se jedná o jednoduchý koncept, je nutná **propracovaná architektura**, aby vše fungovalo tak, jak má. Architektura IoT je skládá nejméně ze **4 vrstev**, a to z vrstvy snímání objektů, vrstvy výměny dat, vrstvy integrace informací a vrstvy aplikačních služeb. Právě v této poslední vrstvě vnímáme užitečnost internetu věcí, neboť jsou v ní zahrnuty chytré aplikace a inteligentní zařízení, která lze použít v mnoha oblastech a učinit je tak „chytřejšími“ – chytré domácnosti, chytré zemědělství, chytrá města, chytré zdravotnictví a mnoho dalších.

Dynamika, inteligence a mobilita internetu věcí z něj činí vysoce poptávanou technologii, ale také jej **dělá zranitelným a rizikovým z hlediska bezpečnosti a ochrany soukromí.** Všechny vrstvy IoT jsou vystavovány různým kybernetickým útokům. **Návrháři chytrých zařízení se proto musí aktivně podílet na vývoji účinných opatření na ochranu soukromí a bezpečí,** a tím posílit internet věcí z hlediska bezpečnosti.

Nicméně, hlavní příčinou zranitelnosti internetu věcí je **nedostatečná informovanost o zajištění bezpečnosti.** Lidé, podniky a společnost jako celek se musí **zapojit do zvyšování gramotnosti v oblasti kybernetické bezpečnosti,** aby bylo možné odstranit příčinu číslo jedna porušování kybernetické bezpečnosti – lidskou chybu.

Mějte toto vše neustále na paměti a zanedlouho se i z Vás stane přeborník na kybernetickou bezpečnost!



Správné odpovědi

Zadání: Co je to internet věcí?

Úkol: Vyberte správné odpovědi: pouze jedna odpověď je správná.

- Internet věcí je síť propojených serverů, které jsou dostupné prostřednictvím internetu.
- Internet věcí je digitalizace a automatizace všech částí společnosti i výrobních procesů.
- Internet věcí je globální síť, která navzájem propojuje počítače po celém světě.
- **Internet věcí je začínající technologie, která se zaměřuje na propojení věcí nebo zařízení navzájem mezi sebou a mezi lidmi nebo uživateli za účelem dosažení některých společných cílů.**

Zadání: Jaké jsou hlavní způsoby využití internetu věcí?

Úkol: Vyberte správné odpovědi: žádná, jedna, jedna a více nebo všechny odpovědi mohou být správně.

- Monitorování elektrického vedení a inteligentní elektrizační soustavy.
- Řízení dodavatelského řetězce v maloobchodě.
- Řízení dodavatelského řetězce v měnícím se průmyslu.
- **Regulace vody v zemědělství.**

Zadání: Která z následujících tvrzení týkajících se zabezpečení IoT zařízení jsou pravdivá?

Úkol: Vyberte správné odpovědi: žádná, jedna, jedna a více nebo všechny odpovědi mohou být správně.

- **Při generování a ukládání dat je vyžadováno zabezpečení dat.**
- Bezpečnostní požadavky na aplikace IoT musí být aplikovány ve třech vrstvách: vrstva aplikačních služeb, vrstva výměny dat a vrstva snímání objektů.
- Pravděpodobnost výskytu phishingového útoku v IoT zařízení je vyšší ve vrstvě integrace informací.
- **Architektura IoT umožňuje škůdcům využít zranitelná místa, která jsou charakteristická pro každou z vrstev internetu věcí.**
- **Škodlivý kód může mít vliv na nejméně tři vrstvy.**

Zadání: Které z následujících tvrzení týkající se ochrany soukromí při užívání IoT zařízení je pravdivé?

Úkol: Vyberte správné odpovědi: pouze jedna odpověď je správná.

- Významný nárůst užití IoT v posledních letech s sebou přinesl několik otázek ohledně bezpečnosti, protože kromě společných a obvyklých vlastností IoT ji ohrožuje snižující se dostupnost dat.
- **Výrobci musí zaručit ochranu osobních údajů uživatelů, které souvisejí s jejich aktivitami, návyky a interakcemi.**
- Soukromí se v tomto případě týká toho, jak dobře se dokážou IoT zařízení bránit před odcizením uživatelských dat.
- Soukromí je ohrožováno pouze ve vrstvě aplikačních služeb.

Zadání: Jaká bezpečnostní opatření byste měli zavést, abyste zabránili kybernetickým útokům na svá IoT zařízení?

Úkol: Vyberte správné odpovědi: žádná, jedna, jedna a více nebo všechny odpovědi mohou být správně.

- a) **Nainstalujte homomorfní šifrování.**



- b) Nainstalujte firewally.
- c) Vytvořte rozptýl nadměrné fragmentace.
- d) Změňte výchozí heslo routeru.
- e) Vypněte na svých chytrých zařízeních funkce, které nepoužíváte.
- f) Deaktivujte vzdálený přístup k Vašemu zařízení.

Zadání: Co dělat, aby se z Vás stal agent 007 kybernetické bezpečnosti?

Úkol: Vyberte správné odpovědi: žádná, jedna, jedna a více nebo všechny odpovědi mohou být správně.

- g) Naučte se programovat, abyste dokázali šifrovat IoT zařízení.
- h) Vypracujte si pohotovostní plán založený na těchto 4 bodech: „Co je generováno?“, „Kde jsou data uložena?“, „Kdy se údaje používají?“ S kým jsou data sdílena?“.
- i) Vypracujte si pohotovostní plán založený na těchto 4 bodech: „Komu zavolat?“, „Jaký bude můj postup?“, „Kdy zalarmovat ostatní?“ a „Které činnosti lze považovat za incidenty?“.
- j) Zapojte celou svou rodinu, kolegy a zaměstnance do povědomí o kybernetické bezpečnosti.
- k) Vypracujte reakční plán až poté, co k nějakému incidentu dojde. Pouze takto jste schopni správně napláňovat, jak v budoucnosti postupovat.