Anna Felkner*

Źródła użytecznych informacji o zagrożeniach w internecie rzeczy

Streszczenie

Jednym z wielu problemów, z jakimi borykają się użytkownicy, producenci czy właściciele sieci oraz osoby na co dzień zajmujące się cyberbezpieczeństwem, jak pracownicy zespołów CSIRT, jest kwestia podatności w urządzeniach internetu rzeczy. Mimo że najpopularniejsze podatności są często przedstawiane dużemu gronu odbiorców, nadal zdecydowana większość z nich jest znana tylko specjalistom od cyberbezpieczeństwa, a nie użytkownikom, którzy to podatne urządzenie mają. Dlatego to właśnie użytkownicy najczęściej mogą być zagrożeni. W związku z tym jest wskazane zwiększenie świadomości użytkowników zagrożeń płynących z posiadania i używania niezabezpieczonych urządzeń, a także zapewnienie dostępu do informacji o podatnościach. Idealnie byłoby mieć jedno źródło, w którym informacje o podatnościach i eksploitach związanych z urządzeniami IoT byłyby zebrane, zagregowane i skorelowane. Nasze obserwacje po analizach wskazały, że wciąż takiego zadowalającego źródła brakowało, dlatego też zdecydowaliśmy się stworzyć repozytorium, w którym informacje o podatnościach i eksploitach mogą być łatwo dostępne dla każdego. W artykule zostały przedstawione m.in. różne źródła użytecznych informacji (actionable information), a także otwarte repozytorium, które w przystępny sposób przedstawia informacje o podatnościach i eksploitach w internecie rzeczy.

Słowa kluczowe: internet rzeczy, IoT, podatność, eksploit, baza informacji o podatnościach i eksploitach, użyteczne informacje

* Anna Felkner, NASK, e-mail: anna.felkner@nask.pl.

Internet rzeczy to koncepcja połączonych ze sobą inteligentnych urządzeń. Koncepcja ta zyskuje coraz większą popularność i stała się rzeczywistością z udziałem każdego z nas. Urządzenia te oferują użytkownikom mnóstwo możliwości w zależności od ich potrzeb. Produkty, które można nazwać inteligentnymi, są ciągle rozwijane i dziś można tak nazwać nie tylko routery, kamery i czujniki bezprzewodowe, lecz także wszelkiego rodzaju inteligentne urządzenia domowe (odkurzacze, pralki, telewizory, lodówki), inteligentne samochody, urządzenia monitorujące zdrowie oraz różnorodne urządzenia przemysłowe – Industrial Control Systems (ICS) i Industrial Internet of Things (IIoT). Biorąc pod uwagę to, że urządzenia internetu rzeczy towarzyszą nam każdego dnia zarówno w życiu prywatnym, jak i zawodowym, zarówno w domu, jak i w przemyśle, zarówno w służbie zdrowia, jak i na ulicach nie możemy pominąć kwestii związanych z ich bezpieczeństwem. Obecny stan bezpieczeństwa urządzeń IoT jest na bardzo niskim poziomie. O ile świadomość w kontekście bezpieczeństwa IT jest stosunkowo wysoka, o tyle świadomość IoT jest wciąż w powijakach. Wielu producentów, często nieświadomie, zaniedbuje ten temat, dlatego że wcześniej nie mieli oni doświadczeń z cyberbezpieczeństwem. W ostatnim czasie, na szczęście, świadomość użytkowników tych urządzeń wzrasta, nadal jednak nie jest to temat w pełni zaspokojony.

Najczęstsze problemy związane z bezpieczeństwem IoT to te, które dotyczą dostępu i szyfrowania. Urządzenia IoT zazwyczaj nie były projektowane z uwzględnieniem bezpieczeństwa jako podstawowej koncepcji. Doprowadziło to do licznych naruszeń sieci domowych i firmowych. Ponadto, jeżeli atakujący ma zdalny dostęp do urządzenia IoT, to może uzyskać dostęp do innych urządzeń IoT w skompromitowanej sieci. Dlatego niezwykle ważna jest ocena zarówno bezpieczeństwa urządzenia, jak i reputacji bezpieczeństwa dostawcy podczas projektowania sieci urządzeń IoT. Jedną z możliwości zabezpieczenia swoich urządzeń IoT jest wdrożenie odrębnej sieci dla sprzętu IoT, odseparowanej i odizolowanej od sieci podstawowej. Drugim niezwykle istotnym aspektem jest aktualizowanie oprogramowania, ograniczanie dostępu fizycznego i logicznego, monitorowanie całej aktywności sieciowej oraz wdrażanie zapór sieciowych i filtrowania ruchu.

Posiadanie informacji o podatnościach (czyli wszelkiego rodzaju lukach w oprogramowaniu lub sprzęcie) i eksploitach (czyli określonym kodzie lub technice wykorzystującej podatność) urządzeń IoT ma kluczowe znaczenie z punktu widzenia właścicieli urządzeń, dostawców usług, właścicieli sieci i producentów urządzeń. Pozyskiwanie tych informacji jest również krytyczne z punktu widzenia krajowych i sektorowych zespołów CSIRT (Zespoły

Reagowania na Incydenty Bezpieczeństwa Komputerowego, Computer Security Incident Response Teams). Zarządzanie podatnościami jest jednym z głównych aspektów bezpieczeństwa zarówno w świecie IT, jak i IoT czy IIoT.

W artykule zostały wykorzystane wyniki badań prowadzonych w ramach projektu Vulnerability and Attack Repository for IoT (VARIoT)[1], w których brały udział następujące osoby: Anna Felkner, Marek Janiszewski, Piotr Lewandowski, Marcin Rytel i Hubert Romanowski. Celem projektu było dostarczenie użytecznych informacji o urządzeniach internetu rzeczy, które mogą być przetwarzane ręcznie lub automatycznie w celu zapewnienia cyberbezpieczeństwa tych urządzeń. W naszej pracy skupiliśmy się na poszukiwaniu informacji o eksploitach i podatnościach w internecie rzeczy i zauważyliśmy, że nie ma jednego źródła, które przedstawiałoby szeroki zakres informacji związanych z tym aspektem bezpieczeństwa. Z naszych badań wynikało, że chociaż informacje były dostępne online, nie było jednego serwisu oferującego dane dotyczące IoT, a samo znalezienie czy wyselekcjonowanie tych informacji nie było trywialne. Krajowe bazy danych o podatnościach zawierają pewne wpisy dotyczące IoT, ale brakuje w nich mechanizmów pozwalających na odróżnienie ich od innych podatności. Co więcej, informacje o wielu podatnościach dotyczących świata internetu rzeczy nigdy nie trafiają do tych baz, ale można je znaleźć rozproszone w internecie, dlatego postanowiliśmy stworzyć takie źródło.

Na początek przeanalizowaliśmy ponad 100 unikalnych źródeł różnego typu. Były to zarówno źródła ustrukturyzowane, które zawierają informacje nie tylko o IoT, lecz także, a raczej przede wszystkim, o ogólnym IT, różne krajowe bazy danych o podatnościach, a także źródła nieustrukturyzowane takie, jak: raporty, blogi czy indywidualne strony internetowe. Z analizy poszczególnych źródeł wynika, że nie istniała jedna, kompleksowa, przeznaczona dla IoT baza danych o podatnościach i eksploitach. Dostępne rozwiązania zostały stworzone z myślą o podatnościach w oprogramowaniu i sprzęcie głównie IT i nie są dobrze przystosowane do zarządzania podatnościami dotyczącymi świata IoT, w którym krzyżuje się wiele domen – sprzęt, oprogramowanie i sieci. Zwykle źródłem informacji o podatnościach są bazy danych o podatnościach. Najpopularniejszą z nich jest baza NVD (National Vulnerability Database)[2], która jest zsynchronizowana z listą CVE (Common Vulnerabilities

1 *Vulnerability and Attack Repository for IoT Project*, https://www.variot.eu [dostęp: 5.01.2023].

2 *National Vulnerability Database*, https://nvd.nist.gov/ [dostęp: 5.01.2023].

and Exposures)[3] i opisuje jedynie podatności z przypisanymi do nich wpisami CVE. Program Common Vulnerabilities and Exposures jest słownikiem zidentyfikowanych podatności. Lista ta pozwala zainteresowanym stronom uzyskać szczegółowe informacje o podatnościach poprzez odwołanie się do unikalnego identyfikatora znanego jako CVE ID. Większość z ogólnych baz podatności nie ma wbudowanej kategoryzacji, która pomogłaby wyselekcjonować z ich zbiorów podatności dotyczące urządzeń IoT. Dlatego wykorzystanie tych baz jako podstawowego źródła do automatycznego zbierania informacji wymaga wcześniejszej wiedzy o tym, które zasoby należą do świata IoT. Rynek urządzeń inteligentnych jest zróżnicowany i szybko rozwijający się, z dużą liczbą producentów, którzy oferują te same produkty pod różnymi markami i nazwami handlowymi. Trudno jest jasno zdefiniować, czym tak naprawdę jest IoT. Ponieważ nie ma jedynej słusznej definicji IoT, więc w naszej pracy przyjęliśmy jako urządzenie IoT określać każdy przedmiot (oprócz telefonu, komputera PC, tabletu i sprzętu centrum danych) wyposażony w łączność sieciową oraz zdolność do gromadzenia i wymiany danych. Wprawdzie smartfony są czasami uważane za urządzenia IoT, lecz zdecydowaliśmy się wyłączyć je z naszej definicji, dlatego że ich stale rosnące możliwości obliczeniowe spowodowały, że łatwiej jest je zaklasyfikować raczej jako komputery przenośne niż proste „rzeczy" podłączone do internetu.

Jak wspomniano wcześniej, istnieje wiele publicznie dostępnych baz danych zawierających różne informacje o podatnościach w różnych typach sprzętu i oprogramowania. Tylko kilka z nich jest poświęconych wyłącznie internetowi rzeczy lub przynajmniej w jakiś sposób wskazuje na takie podatności, ale żadna z nich nie agreguje bezpośrednio informacji z innych źródeł. Poniżej krótko opisano źródła, z których są pobierane dane. Wspomniane wyżej NVD[4] jest ogólną bazą danych o podatnościach prowadzoną przez National Institute of Standards and Technology (NIST). Analizuje i punktuje podatności, które mają nadany unikalny identyfikator CVE. Inną ogólną bazą danych o podatnościach jest China National Vulnerability Database (CNVD)[5] utrzymywana przez chiński krajowy CERT – National Computer Network Emergency Response Technical Team/Coordination Center of China (CNCERT/CC). Jest jedyną spośród narodowych baz podatności, która kategoryzuje podatności

3 *Common Vulnerabilities and Exposures*, https://cve.mitre.org/ [dostęp: 5.01.2023].
4 *National Vulnerability Database*, https://nvd.nist.gov/vuln/search [dostęp: 5.01.2023].
5 *Chinese National Vulnerability Database of Information Security*, http://www.cnnvd.org.cn/ [dostęp: 5.01.2023].

ze względu na rodzaj podatnego produktu i posiada kategorię przeznaczoną dla IoT. Chinese National Vulnerability Database of Information Security (CNNVD)[6] jest bazą podatności utrzymywaną przez chińską agencję rządową – China Information Technology Security Evaluation Center (CNITSEC). Japan Vulnerability Notes iPedia (JVNDB)[7] jest bazą danych o podatnościach prowadzoną przez JPCERT Coordination Center oraz Information-technology Promotion Agency (IPA)[8] z Japonii. Wpisy w bazie są napisane w języku japońskim, ale podzbiór jej danych jest również dostępny w języku angielskim. Baza ICS Vulnerability Database (IVD)[9], obecnie niedostępna, była prowadzona przez chińską firmę Winicssec Technologies i skupiała się wyłącznie na podatnościach występujących w przemysłowych systemach sterowania. Większość jej wpisów stanowiły informacje z NVD, CNVD i CNNVD. Chiński ICS CERT jest częścią CNCERT/CN, opiekuna opisanej wcześniej bazy CNVD. Prowadzi on własną listę podatności[10] skoncentrowaną głównie na podatnościach systemów ICS. Carnegie Mellon University's Software Engineering Institute CERT/CC[11] często publikuje informacje o nowo odkrytych podatnościach, z których część nie znajduje się w NVD. Inne zespoły CERT rzadko zamieszczają na swoich stronach internetowych informacje o podatnościach. Jeżeli nawet są one prezentowane, to podatności dotyczące urządzeń IoT są rzadko spotykane i brakuje ich kategoryzacji. Vulmon jest wyszukiwarką podatności w zabezpieczeniach z bardzo prostym interfejsem[12]. Zero Day Initiative (ZDI) to międzynarodowa inicjatywa prowadzona przez firmę Trend Micro Inc. zajmującą się cyberbezpieczeństwem[13]. Zero Day Initiative odkupuje znalezione podatności od niezależnych badaczy bezpieczeństwa, po czym ujawnia je producentom w celu załatania ich przed upublicznieniem informacji. Zero Science Lab (ZSL) to macedońskie laboratorium badawczo-rozwojowe zajmujące się bezpieczeństwem informacji[14]. Oprócz podatności pozyskujemy też infor-

6 *China National Vulnerability Database*, https://www.cnvd.org.cn/ [dostęp: 5.01.2023].
7 *Japan Vulnerabilities Notes Database*, https://jvndb.jvn.jp/en/ [dostęp: 5.01.2023].
8 *Information-technology Promotion Agency*, https://www.ipa.go.jp/english/ [dostęp: 5.01.2023].
9 *ICS Vulnerability Database*, http://ivd.winicssec.com/ [dostęp: 5.01.2023].
10 *Chinese ICS-CERT website*, https://www.ics-cert.org.cn/portal/index.html [dostęp: 5.01.2023].
11 *Carnegie Mellon University CERT Coordination Center*, https://www.kb.cert.org/vuls/ [dostęp: 5.01.2023].
12 *Vulmon Vulnerability Search Engine*, https://vulmon.com/ [dostęp: 5.01.2023].
13 *Zero Day Initiative*, https://www.zerodayinitiative.com/ [dostęp: 5.01.2023].
14 *Zero Science Lab*, https://www.zeroscience.mk/en/index.php [dostęp: 5.01.2023].

macje o eksploitach z różnych źródeł, m.in. z Exploit DB[15] czy Packet Storm[16]. Źródła zostały dokładniej opisane w pracy Marcina Rytla, Anny Felkner i Marka Janiszewskiego[17].

W artykule przeanalizowano jedynie publicznie dostępne darmowe źródła informacji, co wyklucza płatne serwisy takie, jak m.in. agregator podatności i eksploitów Vulners[18]. Vulners to serwis agregujący informacje dotyczące cyberbezpieczeństwa z wielu źródeł, począwszy od baz danych o podatnościach i ekploitach, poprzez poradniki bezpieczeństwa producentów, aż po blogi związane z bezpieczeństwem. Obecnie dostępne są dane ze 191 źródeł, w tym z niektórych opisanych wcześniej: CNVD, NVD, JVNDB czy ZDI. Jakość i kompletność danych jest różna – często w danych Vulners brakuje części informacji znajdujących się w oryginalnym źródle dla poszczególnych wpisów lub nie wszystkie wpisy z danego źródła są dostępne w Vulners.

Tabela 1. Spis źródeł informacji o podatnościach i eksploitach

Skrót	Nazwa	Typ bazy
CERT CC	Carnegie Mellon University CERT Coordination Center	podatności
CNNVD	Chinese National Database of Information Security	podatności
CNVD	China National Vulnerability Database	podatności
Exploit-DB	Exploit Database by Offensive Security	eksploity
ICS-CERT CN	Chinese ICS-CERT website	podatności
IVD	ICS Vulnerability Database	podatności
JVNDB	Japan Vulnerabilities Notes Database	podatności
NVD	National Vulnerability Database	podatności
Packet Storm	Packet Storm Security	podatności/eksploity
Vulmon	Vulmon Vulnerability Search Engine Vulnerability	podatności
ZDI	Zero Day Initiative	podatności
ZSL	Zero Science Lab	podatności

Ponieważ wiele podatności i eksploitów dotykających urządzenia IoT nigdy nie zostaje skatalogowane w bazach danych, więc jest konieczne przeglądanie dodatkowych źródeł, żeby zachować świadomość krajobrazu zagrożeń

15 *Offensive Security's Exploit Database Archive*, https://www.exploit-db.com/ [dostęp: 5.01.2023].

16 *Packet Storm*, https://packetstormsecurity.com/ [dostęp: 5.01.2023].

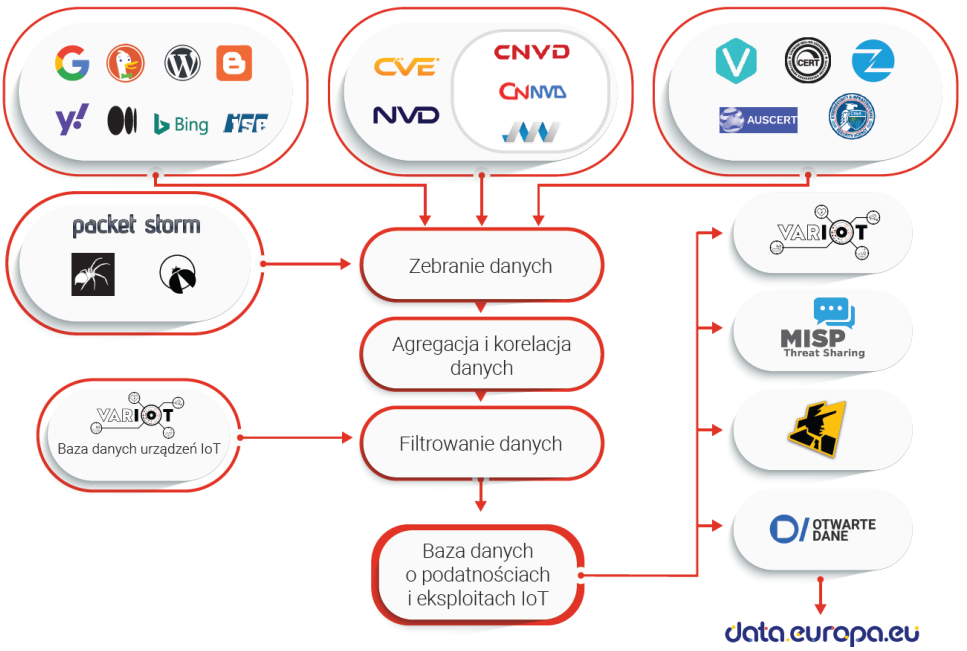
17 M. Rytel, A. Felkner, M. Janiszewski, *Towards a Safer Internet of Things – A Survey of IoT Vulnerability Data Sources*, „Sensors" 2020, t. 20, nr 21.

18 *Vulners – Vulnerability Database*, https://vulners.com/ [dostęp: 5.01.2023].

IoT. Oprócz wpisów zebranych ze źródeł ustrukturyzowanych wymienionych w tabeli 1 szukaliśmy również najnowszych postów i artykułów pojawiających się w internecie. Dobrym źródłem są blogi, ale trudno je śledzić i wyciągać z nich istotne informacje. Są one pisane przez indywidualnych badaczy, grupy hakerskie lub firmy zajmujące się bezpieczeństwem, prezentujących swoje osiągnięcia w hakowaniu inteligentnych urządzeń. Ponieważ rzadko są one poświęcone wyłącznie temu tematowi, więc poszczególne posty związane z IoT trzeba filtrować. W przypadku tego rodzaju źródeł odpowiednie metadane można wyodrębnić z surowego tekstu. Jedną z unikalnych cech zbudowanej bazy podatności VARIoT jest korelacja i agregacja informacji o podatnościach z różnych publicznie dostępnych źródeł.

Cały proces tworzenia bazy podatności i eksploitów IoT, którą przygotowaliśmy w trakcie realizacji projektu VARIoT (zob. rys. 1), można przedstawić w kilku fazach. W pierwszej została przeprowadzona identyfikacja i selekcja wartościowych źródeł informacji związanych z podatnościami i eksploitami. Przedmiotem zainteresowania są tu zarówno ustrukturyzowane źródła (z których łatwiej jest pobrać dane), jak i nieustrukturyzowane, takie jak blogi czy indywidualne strony internetowe (z których pobieranie danych jest zwykle bardziej skomplikowane, ale mogą one dostarczać informacji wyprzedzających oficjalne bazy danych lub zawierać zupełnie unikalne dane). W drugim etapie zbieraliśmy informacje z tych źródeł, w trzecim informacje te były standaryzowane, w czwartym – informacje z różnych źródeł na temat danej podatności lub eksploita były korelowane i agregowane. Piąty polega na wzbogaceniu i wyborze najbardziej wiarygodnych informacji o każdej podatności i eksploicie. Na podstawie informacji zawartych w bazie danych oraz uzyskanych od konsorcjantów projektu VARIoT przygotowaliśmy słowniki informacji o producentach, modelach i typach urządzeń oraz o typach podatności. Słowniki te zostały wykorzystane jako słowa kluczowe do wyszukiwania w tekście oraz jako zbiory danych treningowych dla innych metod. Ocena zaufania ma na celu wybór najbardziej wiarygodnej i informacyjnej części informacji, ocenę wiarygodności informacji oraz identyfikację podatności i eksploitów związanych z IoT. Odbywa się to na podstawie reputacji źródła, zbieżności informacji z różnych źródeł, metody agregacji i klasyfikacji oraz dodatkowych wyszukiwań. Stworzona w opisany powyżej sposób baza danych może być następnie udostępniana i wykorzystywana przez różne podmioty do różnych celów. Wyszukiwanie informacji związanych z IoT odbywa się również poprzez filtrowanie na różnych

poziomach z wykorzystaniem stworzonej przez nas taksonomii urządzeń IoT, wewnętrznego katalogu urządzeń IoT, mechanizmu filtrowania na podstawie słów kluczowych itp.[19].



Źródło: NASK-PIB.

Rys. 1. Sposób tworzenia bazy danych podatności

Stworzenie uporządkowanej, publicznie dostępnej bazy danych zawierającej informacje o znanych podatnościach technicznych i eksploitach jest niezwykle korzystne dla wszystkich interesariuszy: użytkowników, producentów i właścicieli sieci, a także zespołów CSIRT czy innych osób zajmujących się bezpieczeństwem urządzeń i oprogramowania. Zbadaliśmy duży przekrój różnego rodzaju źródeł i na tej podstawie możemy stwierdzić, że zbierając dane z wielu źródeł, możemy uzyskać bardziej kompletny i wyczerpujący wpis na temat danej luki lub eksploita niż z jednego źródła. Ponieważ przeszukujemy wiele różnych typów publicznie dostępnych źródeł, a nasza baza danych koreluje i agreguje dane z tych źródeł, więc sprawia to, że każdy wpis jest bogaty

19 Szczegółowy opis etapów zob. M. Janiszewski, A. Felkner, P. Lewandowski, M. Rytel, H. Romanowski, *Automatic Actionable Information Processing and Trust Management towards Safer Internet of Things*, „Sensors" 2021, t. 21, nr 13.

w informacje, które mogą być wykorzystane do zapewnienia bezpieczeństwa urządzeń IoT, a także zmniejsza ryzyko pominięcia niektórych danych lub opóźnień w uzyskaniu informacji o konkretnych podatnościach.

Stworzona przez nas baza informacji o podatnościach i eksploitach IoT została opublikowana na stronie https://www.variotdbs.pl/. Strona dostępna jest w dwóch językach (angielskim i polskim), a szczegółowe informacje dotyczące podatności i eksploitów dostępne są tylko w języku angielskim. Główne sekcje, które można znaleźć na stronie, to:

1) podatności – tutaj przedstawione są luki bezpieczeństwa dotykające urządzeń IoT. Sekcja ta umożliwia przeglądanie najnowszych podatności IoT oraz ich wyszukiwanie. Wyszukiwanie podatności jest możliwe z wykorzystaniem atrybutów zarówno według producenta, modelu urządzenia i jego wersji, identyfikatora CVE, identyfikatora VARIoT, numeru CWE (Common Weakness Enumeration[20]) oraz typu, jak i dowolnej frazy opisującej podatność. Takie wyszukiwanie daje wiele możliwości, dlatego że można znaleźć opis podatności, wykorzystując dowolne z powyższych pól, np. typ urządzenia, oraz inne powiązane źródła informacji o podatnościach. Każdy wpis składa się z danych dotyczących konkretnej podatności znalezionych z różnych źródeł, zawiera źródła informacji i obliczone poziomy zaufania, a także zagregowane linki do zewnętrznych źródeł, z którymi można zapoznać się w celu uzyskania dalszych informacji;

2) eksploity – tutaj prezentowane są publicznie dostępne eksploity wymierzone w urządzenia IoT. Sekcja ta pozwala na przeglądanie eksploitów, które mogą zagrażać urządzeniom IoT. Działa ona w podobny sposób jak sekcja „podatności", czyli też można szukać informacji o eksploitach według producenta, modelu czy wersji urządzenia;

3) wiadomości – tutaj można zobaczyć automatycznie generowaną listę wiadomości na temat bezpieczeństwa IoT, które to wiadomości zostały zebrane przy użyciu wyszukiwarki wykorzystującej autorskie skrypty do filtrowania wyników wyszukiwania. Sekcja ta pokazuje różnego rodzaju informacje związane z podatnościami w świecie internetu rzeczy. Wiadomości są zbierane z różnych źródeł, głównie nieustrukturyzowanych, takich, jak: raporty, blogi, informacje dostarczane przez osoby zajmujące się badaniem podatności lub w jakikolwiek sposób związane z cyberbezpieczeństwem.

20 *Common Weakness Enumeration*, https://cwe.mitre.org/ [dostęp: 5.01.2023].

4) API – tutaj znajduje się opis jak w prosty sposób pobrać dane, które udostępniamy na stronie poprzez API. Można to zrobić za pomocą jednego z dwóch formatów plików, tj. JSON i JSON-LD;

5) ontologia – tutaj znajduje się opis ontologii wpisów do baz podatności i eksploitów VARIoT (tylko w języku angielskim).

Bazy danych podatności i eksploitów budowane są na podstawie wcześniej opisanych źródeł. Wyszukiwarka wiadomości korzysta z wielu dostępnych wyszukiwarek internetowych i na podstawie znalezionych w ten sposób informacji tworzy wpis przedstawiający dodatkowe informacje o podatnościach i urządzeniach, które pozyskiwane są za pomocą przetwarzania języka naturalnego (Natural Language Processing – NLP), uczenia maszynowego (Machine Learning – ML) i sztucznej inteligencji (Artificial Intelligence – AI) oraz specjalnie do tego przygotowanych filtrów w celu lepszego dostosowania wpisu i połączenia danych uzyskanych z wielu źródeł. Opracowany mechanizm jest w stanie wydobyć informacje z nieustrukturyzowanych źródeł informacji takich, jak: blogi, raporty i artykuły. Ponadto oblicza zaufanie do wybranych informacji, żeby lepiej ocenić ich istotność. W kontekście bazy danych podatności i eksploitów zaufanie opiera się na punktacji wiarygodności źródeł ustalonej na podstawie naszej wiedzy o tych źródłach, a w kontekście wiadomości – na informacjach wyodrębnionych ze znalezionych wpisów, tj. słowa kluczowe, nazwy producentów i produktów, typy podatności oraz linki do znanych baz danych podatności[21].

Wraz z gwałtownym wzrostem wykorzystania produktów IoT w różnorodnych zastosowaniach ich bezpieczeństwo staje się coraz większym problemem. Duża liczba podatności w zabezpieczeniach w połączeniu z brakiem wystarczającego wsparcia dla produktów i procesów łatania zagraża gospodarce, bezpieczeństwu obywateli i ich prywatności. Niezabezpieczone urządzenia IoT już teraz są wykorzystywane w masowych atakach, które mogą stać się jeszcze większe i częstsze, jeżeli nie zostaną podjęte działania mające na celu zabezpieczenie środowiska IoT. Publicznie dostępne źródło uporządkowanych informacji o znanych podatnościach i eksploitach w urządzeniach IoT to wielki krok w kierunku poprawy bezpieczeństwa tych urządzeń. Jak dotąd, żadne z istniejących rozwiązań nie było zadowalające, co podkreślało potrzebę stworzenia bazy danych skoncentrowanej na IoT. Przygotowane przez nas

21 Więcej na ten temat zob. A. Felkner, M. Rytel, *A Repository of Actionable Information on the Internet of Things* [w:] *Proceedings of the 19th International Conference on Wireless Networks and Mobile Systems*, t. 1, [Lizbona] 2022, s. 69–75.

repozytorium jest publicznie dostępne na poświęconej jej stronie[22], za pośrednictwem Europejskiego Portalu Danych[23] oraz krajowych Portali Danych (jak polski Portal Otwartych Danych[24]), a także innych źródeł, jak Malware Information Sharing Platform (MISP), która jest powszechnie wykorzystywana przez społeczność analityków cyberbezpieczeństwa oraz za pośrednictwem sieci dystrybucji organizacji ShadowServer, dzięki której dane są raportowane do krajowych zespołów reagowania na incydenty bezpieczeństwa komputerowego i zweryfikowanych właścicieli sieci.

Bibliografia

Felkner A., Rytel M., *A Repository of Actionable Information on the Internet of Things* [w:] *Proceedings of the 19th International Conference on Wireless Networks and Mobile Systems*, t. 1, [Lizbona] 2022.

Janiszewski M., Felkner A., Lewandowski P., Rytel M., Romanowski H., *Automatic Actionable Information Processing and Trust Management towards Safer Internet of Things*, „Sensors" 2021, t. 21, nr 13.

Rytel M., Felkner A., Janiszewski M., *Towards a Safer Internet of Things — A Survey of IoT Vulnerability Data Sources*, „Sensors" 2020, t. 20, nr 21

Sources of actionable information about threats on the Internet of Things

Abstract

One of the many problems facied by users, producers or network owners as well as those who deal with cybersecurity on a daily basis is the issue of vulnerabilities in Internet of Things devices. Although the most popular vulnerabilities are often presented to the general public, the vast majority of them are still known only to cybersecurity specialists, and not to the users who own the vulnerable device. Consequently, it is the users who are most likely to be at risk. It is advisable to increase user awareness of the dangers of owning and using unsecured devices as well as provide access to information about vulnerabilities. Ideally, we would like to have a single source where information about vulnerabilities and exploits related to IoT devices would be collected, aggregated and correlated. Among other things, the article presents various sources of actionable information as well as an open repository that presents information about vulnerabilities and exploits in an accessible way.

Key words: Internet of Things, IoT, vulnerability, exploit, vulnerability and exploit database, actionable information

22 *VARIoT baza podatności i eksploitów IoT*, https://www.variotdbs.pl/ [dostęp: 5.01.2023].
23 https://data.europa.eu.
24 https://dane.gov.pl/.