ANALIZA RISCURILOR ȘI AMENINȚĂRILOR DE SECURITATE ALE DISPOZITIVELOR IoT

Mihaela MĂMĂLIGĂ

Departamentul Telecomunicaţii şi Sisteme Electronice, grupa RST-181, Facultatea Electronică şi Telecomunicaţii, Universitatea Tehnică a Moldovei, Chişinău, Republica Moldova

Autor corespondent:Alexei Arina, arina.alexei@tse.utm.md

Rezumat. *Securitatea IoT se referă la metodele de protecție utilizate pentru a securiza dispozitivele conectate la internet sau bazate pe rețea. IoT implică adăugarea de conectivitate la internet la un sistem de dispozitive de calcul interconectate, mașini mecanice și digitale, obiecte, animale și/sau oameni. Fiecărui „lucru" i se oferă un identificator unic și capacitatea de a transfera automat date printr-o rețea. Permiterea dispozitivelor să se conecteze la internet le deschide la o serie de vulnerabilități grave dacă nu sunt protejate corespunzător. Astfel, analizând tipurile de riscuri IoT și problemele de securitate cu care se confruntă dispozitivele IoT, au fost elaborate practici pentru a reduce riscurile și a preveni amenințările.*

Cuvinte cheie*: Securitatea IoT, riscuri IoT, vulnerabilități, securizare.*

Introducere

Securitatea Internet of Things (IoT) este un set de abordări și practici pentru protejarea dispozitivelor fizice, rețelelor, proceselor și tehnologiilor care cuprind un mediu IoT împotriva unui spectru larg de atacuri de securitate IoT. Securitatea IoT este familia de tehnici, strategii și instrumente utilizate pentru a proteja aceste dispozitive împotriva compromisurilor. În mod ironic, conectivitatea inerentă IoT face aceste dispozitive din ce în ce mai vulnerabile la atacurile cibernetice [3].

Deoarece IoT este atât de larg, securitatea IoT este și mai largă. Acest lucru a dus la o varietate de metodologii care intră sub umbrela securității IoT. Securitatea interfeței programului de aplicație (API) , autentificarea infrastructurii cu chei publice (PKI) și securitatea rețelei sunt doar câteva dintre metodele pe care liderii IT le pot folosi pentru a combate amenințarea tot mai mare a criminalității cibernetice și a terorismului cibernetic înrădăcinată în dispozitivele IoT vulnerabile [4].

Conform unui studiu efectuat de Gartner , 50 de miliarde de dispozitive conectate și alți senzori vor fi utilizați în întreaga lume până în 2025:

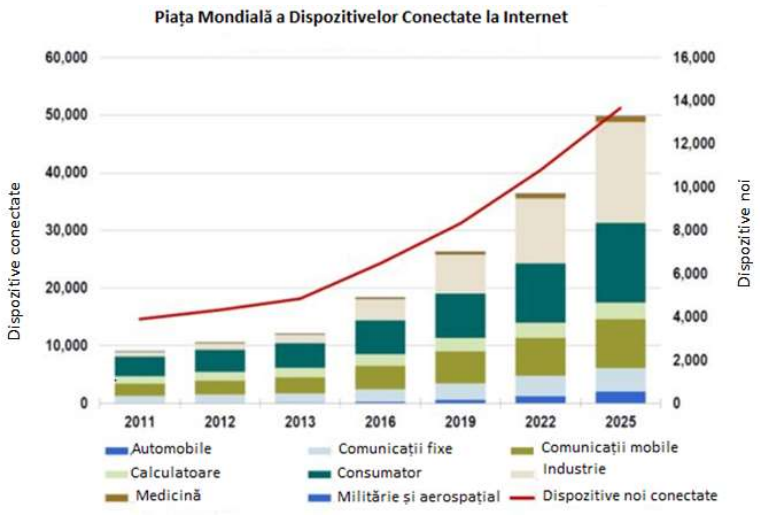

Figura 1. Utilizarea dispozitivelor IoT în viitorul apropiat

1. Tipuri de riscuri IoT

Multe domenii, inclusiv finanțe, lanț de aprovizionare și asistență medicală, sunt afectate de atacurile IoT. Dacă vulnerabilitățile din dispozitivele IoT (sau mediul IoT) sunt exploatate de amenințări din sistem, aceasta duce la riscuri IoT și anume:

1. Risc etic IoT: se referă la efectele adverse neprevăzute ale acțiunilor neetice care utilizează dispozitive IoT. Volkswagen, o companie producătoare de automobile, a dezvoltat și instalat software pentru a înșela testele de emisii diesel. Acest lucru a încălcat Legea privind aerul curat al SUA, a compromis standardele organizației și ale industriei și a dus la pierderi masive de reputație și financiare.
2. Risc IoT de securitate și confidențialitate: se referă la exploatarea vulnerabilităților din sistem pentru a obține acces la active cu intenția de a provoca prejudicii. În octombrie 2016, Botnet-ul Mirai (malware specializat IoT) a lansat un atac DdoS asupra DYN care a dus la căderea unor părți ale internetului și a afectat Twitter, Netflix, CNN, Reddit și multe altele. Această categorie include și riscul de confidențialitate IoT care se referă la pierderea temporară sau permanentă a controlului datelor care dăunează organizației. Încălcarea datelor eBay care a avut loc în luna mai 2014 a determinat piratarea înregistrărilor clienților săi, inclusiv a parolelor.
3. Risc tehnic IoT: Acest lucru se datorează defecțiunilor hardware sau software din cauza designului, evaluării proaste etc. S-a descoperit recent că cipurile de computere personale create în ultimii 20 de ani conțin defecte de securitate la nivel de cip. Meltdown este o vulnerabilitate hardware a microprocesorului Intel ×86 care permite unei metode necinstite să citească toată memoria, deși nu este autorizată să facă acest lucru. Problemele de design slabe duc la riscuri IoT pentru confidențialitate și securitate. [1]

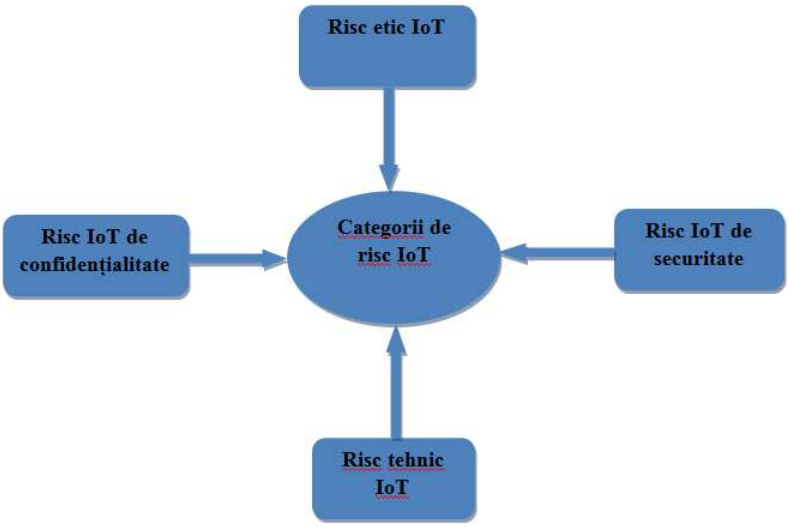

Figura 2. Categorii de risc IoT

2. Problemele de securitate în IoT

Securitatea IoT este critică în mare parte din cauza suprafeței de atac extinse a amenințărilor care au afectat deja rețelele. La aceste amenințări se adaugă practicile nesigure în rândul utilizatorilor și organizațiilor care nu au resursele sau cunoștințele necesare pentru a-și proteja cel mai bine ecosistemele IoT.

Aceste probleme de securitate include următoarele:

- **Vulnerabilități.** Vulnerabilitățile sunt o problemă mare care afectează în mod constant utilizatorii și organizațiile. Unul dintre principalele motive pentru care dispozitivele IoT sunt vulnerabile este faptul că nu au capacitatea de calcul pentru securitatea încorporată. Un alt motiv pentru care vulnerabilitățile pot fi atât de răspândite este bugetul limitat pentru dezvoltarea și testarea firmware-ului securizat, care este influențat de prețul dispozitivelor și de ciclul lor de dezvoltare foarte scurt. Pe lângă dispozitivele în sine, vulnerabilitățile din aplicațiile web și software-ul asociat pentru dispozitivele IoT pot duce la sisteme compromise [2].

- **Programe malware.** În ciuda capacității limitate de calcul a majorității dispozitivelor IoT, acestea pot fi în continuare infectate cu malware. Acesta este ceva ce infractorii cibernetici l-au folosit cu mare efect în ultimii ani. Malware-ul botnet IoT se numără printre variantele cele mai frecvent întâlnite, deoarece sunt atât versatile, cât și profitabile pentru infractorii cibernetici. Cel mai notabil atac a fost în 2016, când Mirai a distrus site-uri web și servicii importante folosind o armată de dispozitive IoT obișnuite. Alte familii de programe malware include programe malware și ransomware pentru extracția de criptomonede .
- **Escaladarea atacurilor cibernetice.** Dispozitivele infectate sunt adesea folosite pentru atacuri distribuite de refuzare a serviciului (DdoS). Dispozitivele deturnate pot fi, de asemenea, folosite ca bază de atac pentru a infecta mai multe mașini și a masca activitățile rău intenționate sau ca punct de intrare pentru mișcarea laterală într-o rețea corporativă. În timp ce organizațiile pot părea ținte mai profitabile, casele inteligente înregistrează și un număr surprinzător de atacuri cibernetice neprevăzute .
- **Furtul de informații și expunerea necunoscută.** Ca și în orice lucru care are de-a face cu internetul, dispozitivele conectate cresc șansele de expunere online. Informațiile tehnice importante și chiar personale pot fi stocate și vizate în neștiință în aceste dispozitive.
- **Gestionarea defectuoasă a dispozitivului și configurarea greșită.** Supravegherile de securitate, igiena proastă a parolelor și gestionarea defectuoasă a dispozitivului pot contribui la succesul acestor amenințări. De asemenea, utilizatorii pot să nu aibă cunoștințele și capacitatea de a implementa măsuri de securitate adecvate, în care furnizorii de servicii și producătorii ar putea avea nevoie să-și ajute clienții să obțină o protecție mai bună [5].

3. Recomandări de securitate IoT

Nu există nici o remediere instantanee care să poată răspunde problemelor de securitate și amenințărilor prezentate în acest articol. Pot fi necesare strategii și instrumente specifice pentru a securiza în mod corespunzător sisteme și aspecte mai specializate ale IoT. Cu toate acestea, utilizatorii pot aplica câteva bune practici pentru a reduce riscurile și a preveni amenințările:

- **Atribuirea unui administrator al dispozitivelor IoT.** Faptul că o persoană acționează ca administrator al dispozitivelor IoT și al rețelei poate ajuta la minimizarea observărilor și expunerilor de securitate. Aceștia vor fi responsabili cu asigurarea securității dispozitivelor IoT , chiar și acasă. Rolul este esențial mai ales în această perioadă de configurare a WFH, unde experții IT au un control limitat în securizarea rețelelor de acasă care au acum o influență mai puternică asupra rețelelor de lucru.
- **Verificarea în mod regulat a patch-urilor și actualizărilor.** Vulnerabilitățile reprezintă o problemă majoră și constantă în domeniul IoT. Acest lucru se datorează faptului că vulnerabilitățile pot proveni de la orice strat de dispozitive IoT. Chiar și vulnerabilitățile mai vechi sunt încă folosite de infractorii cibernetici pentru a infecta dispozitivele, demonstrând cât de mult pot rămâne online dispozitivele nepatchate.
- **Utilizarea parolelor puternice și unice pentru toate conturile.** Parolele puternice ajută la prevenirea multor atacuri cibernetice. Managerii de parole pot ajuta utilizatorii să creeze parole unice și puternice pe care utilizatorii le pot stoca în aplicație sau software în sine.
- **Prioritizarea securității Wi-Fi.** Unele dintre modalitățile prin care utilizatorii pot face acest lucru includ activarea paravanului de protecție a routerului, dezactivarea WPS și activarea protocolului de securitate WPA2 și utilizarea unei parole puternice pentru accesul Wi-Fi. Asigurarea setărilor securizate ale routerului este, de asemenea, o parte importantă a acestui pas.
- **Monitorizarea rețelei de referință și comportamentului dispozitivului.** Atacurile cibernetice pot fi dificil de detectat. Cunoașterea comportamentului de bază (viteza, lățimea de bandă tipică etc.) al dispozitivelor și al rețelei poate ajuta utilizatorii să urmărească abaterile care sugerează infecții cu malware.

- **Aplicarea segmentării rețelei.** Utilizatorii pot minimiza riscul atacurilor legate de IoT prin crearea unei rețele independente pentru dispozitivele IoT și a alta pentru conexiunile pentru oaspeți. Segmentarea rețelei ajută, de asemenea, la prevenirea răspândirii atacurilor și la izolarea eventualelor dispozitive problematice care nu pot fi scoase imediat offline.
- **Securizarea rețelei pentru a consolida securitatea.** Dispozitivele IoT pot pune rețelele în pericol, dar rețelele pot servi și ca teren nivelat prin care utilizatorii pot implementa măsuri de securitate care acoperă toate dispozitivele conectate.
- **Securizarea convergenții IoT-cloud și aplicarea soluțiilor bazate pe cloud.** IoT și cloud-ul devin din ce în ce mai integrate. Este important să ne uităm la implicațiile de securitate ale fiecărei tehnologii pentru cealaltă. Soluțiile bazate pe cloud pot fi, de asemenea, luate în considerare pentru a oferi securitate suplimentară și capabilități de procesare dispozitivelor de vârf IoT.
- **Luarea în considerare a soluțiilor și instrumentelor de securitate.** Un obstacol mare cu care se confruntă utilizatorii în încercarea de a-și securiza ecosistemele IoT este capacitatea limitată în care pot implementa acești pași. Unele setări ale dispozitivului ar putea avea acces restricționat și sunt dificil de configurat. În astfel de cazuri, utilizatorii își pot completa eforturile luând în considerare soluții de securitate care oferă protecție pe mai multe straturi și criptare endpoint.
- **Luarea în considerare a diferitor protocoale utilizate de dispozitivele IoT.** Pentru a comunica, dispozitivele IoT folosesc nu numai protocoale de internet, ci și un set imens de protocoale de rețea diferite, de la binecunoscutele Bluetooth și Near Field Communication (aka NFC), la cele mai puțin cunoscute nRF24, nRFxx, 443MHz, LoRA, LoRaWAN și comunicații optice, în infraroșu. Administratorii trebuie să înțeleagă întregul set de protocoale utilizate în sistemele lor IoT pentru a reduce riscurile și a preveni amenințările.
- **Asigurarea utilizării intensivă a GPS-ului.** Unele dispozitive și aplicații IoT folosesc în mare măsură GPS-ul, ceea ce are potențiale probleme de securitate. Organizațiile, în special, trebuie să fie atenți la cazurile în care semnalele GPS pot fi blocate sau chiar falsificate, mai ales dacă folosesc sisteme de poziționare pentru producție, monitorizare și alte funcții. Dacă aceste sisteme de poziționare sunt cruciale pentru o companie, atunci ar trebui să existe și mijloace de monitorizare a semnalului GPS în companie [5].

Concluzii

Securitatea IoT, include o gamă largă de tehnici , strategii, protocoale și acțiuni care urmăresc atenuarea vulnerabilităților IoT în creștere ale afacerilor moderne. Orice vulnerabilitate poate duce la o defecțiune a sistemului sau la un atac de hacking, care, la rândul său, poate afecta sute sau mii de oameni. Un alt motiv important pentru a acorda prioritate securității atunci când se dezvoltă sisteme IoT este păstrarea datelor în siguranță. Dispozitivele inteligente adună tone de date sensibile, inclusiv informații de identificare personală, care trebuie să fie protejate de diverse legi, standarde și reglementări de securitate cibernetică. Compromisul unor astfel de informații poate duce la procese și amenzi. De asemenea, poate duce la deteriorarea reputației și la pierderea încrederii clienților.

Cele mai importante probleme de securitate sunt legate, fără îndoială, de controlul accesului și serviciile expuse. În plus, dispozitivele IoT ar trebui să implementeze măsuri de securitate de cele mai bune practici, cum ar fi criptarea. Furnizorii pot facilita utilizarea în siguranță a produselor lor prin furnizarea de documentație și interacțiunea cu utilizatorii și profesioniștii în securitate. Pentru a îngreuna atacatorii, dispozitivele ar trebui să fie securizate fizic. În cele din urmă, dacă un dispozitiv este compromis, acesta ar trebui să respingă programele furnizate de atacator și să notifice utilizatorul că ceva nu este în regulă.

Referinţe

1. Kandasamy, K., Srinivas, S., Achuthan, K. *et al.* IoT cyber risk: a holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process. *EURASIP J. on Info. Security* **2020,** 8 (2020). https://doi.org/10.1186/s13635-020-00111-0
2. Alexei, A., & Alexei, A. (2021). Analysis of IoT security issues used in Higher Education Institutions. *INTERNATIONAL JOURNAL OF MATHEMATICS AND COMPUTER RESEARCH*, *09*(05). https://doi.org/10.47191/ijmcr/v9i5.01
3. Anna Katrenko, Elena Semeniak, Internet of Things (IoT) Security: Challenges and Best Practices. Disponibil: https://www.apriorit.com/dev-blog/513-iot-security
4. Sharon Shea, Ivy Wigmore, IoT security (internet of things security). Disponibil: https://internetofthingsagenda.techtarget.com/definition/IoT-security-Internet-of-Things-security
5. IoT Security Issues, Threats, and Defenses. Disponibil: https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/iot-security-101-threats-issues-and-defenses