Soluții pentru implementarea funcțiilor de securitate în cazul aplicațiilor tipice în medii SMART

Mihail DUMITRACHE[1,2], Ionuț-Eugen SANDU[1,3], Ionuț PETRE[1,3]

[1] Institutul Național de Cercetare-Dezvoltare în Informatică – ICI București
[2] Universitatea din București – Facultatea de Litere
[3] Universitatea „Lucian Blaga“ din Sibiu

mihail.dumitrache@ici.ro, ionut.sandu@ici.ro, ionut.petre@ici.ro

Rezumat: Soluțiile privind funcțiile de securitate în cazul aplicațiilor tipice în medii Smart ar trebui să fie implementate de producătorii care fabrică dispozitive IoT (Internet of Things), de inginerii care proiectează soluții IoT, de cercetătorii care evaluează sisteme IoT și de cei care caută să reglementeze utilizarea lor în condiții de siguranță. Această listă de bune practici prezentate nu își propune să fie una exhaustivă, ci reprezintă, mai degrabă, tipurile de activități despre care considerăm că vor duce la o securitate IoT îmbunătățită. Folosirea unui software de securitate dedicat pentru ecosistemul IoT contribuie decisiv la restrângerea accesului sau manipularea dispozitivelor inteligente conectate, la asigurarea transferului, gestionarea și securitatea datelor de pe dispozitivele IoT, la primirea de informații cu privire la amenințările sau vulnerabilitățile emergente, la primirea de actualizări regulate de securitate atât pentru dispozitivele IoT, cât și pentru hub-urile de gestionare ale dispozitivelor IoT, precum și la îmbunătățirea eficientă și creșterea beneficiilor legate de funcționarea IoT. Acest studiu prezintă un exemplu de perspectivă inginerească asupra tipurilor de proceduri care constituie o securitate IoT eficientă.

Cuvinte cheie: Soluții de securitate, Internet of Things, IoT, medii Smart, securitatea rețelelor.

Solutions for implementing security features for typical applications in SMART environments

Abstract: The solutions on security functions for typical applications in Smart environments should be implemented by providers who manufacture IoT (Internet of Things) devices, by engineers designing IoT solutions, by researchers evaluating IoT systems and by those seeking to regulate their safe use. This list of good practices is not intended to be exhaustive, rather they represent the types of activities that we believe will lead to improved IoT security. The use of dedicated security software for the IoT ecosystem makes a decisive contribution to restricting access or manipulating connected smart devices, to ensure the transfer, data management and security on IoT devices, receiving information on emerging threats or vulnerabilities, receiving regular security updates for both IoT devices and IoT device management hubs and to effectively improve and increase the benefits of IoT operation. This study presents an example of an engineering perspective on the types of procedures that constitute effective IoT security.

Keywords: Security solutions, Internet of Things, IoT, Smart environments, network security.

1. Introducere

Tehnologia IoT (Internet of Things) este într-o creștere continuă la nivel internațional, astfel încât a devenit omniprezentă în viața noastră, fiind caracterizată de o mulțime de aplicații și de lipsa unor politici de securitate unitare. Pentru a implementa cele mai potrivite soluții de securitate trebuie analizate și înțelese principalele tipuri de amenințări din acest domeniu, precum și modul de înlăturare a acestor amenințări. Open Web Application Security Project (OWASP), care este o comunitate online și dezvoltă metodologii, documentații, instrumente și tehnologii disponibile în mod gratuit în domeniul securității aplicațiilor web, a publicat o listă cu primele zece tipuri de vulnerabilități în domeniul IoT (The OWASP IoT Security Team, 2018). Acestea sunt: parole slabe, intuibile sau care nu se pot schimba; servicii de comunicare nesigure; interfețe de conectare nesigure; lipsa mecanismelor de actualizare; utilizarea componentelor nesigure sau depășite; protecție insuficientă a confidențialității; transfer și stocare nesigură a datelor; lipsa gestionării centralizate/unitare a dispozitivelor; setări implicite nesigure; lipsa întăririi fizice.

https://doi.org/10.33436/v31i2y202109

Pentru a proteja consumatorii și publicul, profesioniștii din domeniul tehnic, autoritățile legislative și alți decidenți politici trebuie să definească și să încurajeze practici adecvate de securitate și confidențialitate. Securitatea informațiilor este despre ce trebuie protejat, de ce trebuie protejat și cum să fie asigurată protecția (Cîrnu et al., 2018.). În prezent, dat fiind faptul că în circumstanțe diferite se impun măsuri de precauție diferite, nu este posibilă definirea unui set de reguli universale pentru securitatea IoT. Cu toate acestea, este posibilă creionarea unui set de principii generale sau de bune practici. Prin noțiunea de „bune practici" înțelegem măsuri de securitate sau confidențialitate acceptate la scară largă de profesioniști din domeniul tehnic ca fiind benefice sau necesare. Intenția noastră nu este să sugerăm că o măsură anume este mai bună decât oricare alta. În aplicarea bunelor practici trebuie ținut seama că simplificarea securității informațiilor pentru angajați este esențială, astfel încât politicile de securitate să fie înțelese și aplicate până la cele mai elementare activități (Banciu et al., 2020).

2. Bune practici privind securizarea echipamentelor

2.1. Hardware-ul rezistent la tampering (manipulare)

Unele dispozitive IoT pot funcționa în mod continuu fără a fi monitorizate și fără a se supune nivelului de securitate pe care îl implică această supraveghere umană directă și constantă, deși este ideală menținerea dispozitivelor relativ izolate, astfel încât numai anumite persoane special desemnate să poată avea acces fizic la ele. În special, în cazul dispozitivelor complet nesupravegheate ar putea fi util ca acestea să fie rezistente la tampering. Această formă de consolidare a dispozitivului IoT poate ajuta la blocarea accesului la date din partea unor potențiali intruși. De asemenea, poate asigura protecție împotriva unui hacker care ar putea să cumpere dispozitive pentru a le folosi ca armă în alte atacuri.

Securitatea fizică a punctelor terminale poate include, de exemplu, mici dispozitive simple din plastic, protecții pentru porturi și pentru camera web care blochează porturile USB și Ethernet sau acoperă fereastra camerei web. Dispozitivele de blocare a porturilor împiedică pătrunderea programelor de tip malware. Unele metode de blocare a accesului dezactivează dispozitivul în momentul în care se încearcă coruperea acestuia. Consolidarea punctului terminal, ca metodă de bune practici, implică, o abordare stratificată ce le impune atacatorilor să ocolească o varietate de obstacole gândite să protejeze dispozitivul și datele stocate împotriva accesului și utilizării lor ilegale. La nivel de hardware/software de inițializare, metode sigure ar putea fi niște parole puternice la inițializare sau stabilirea condiției ca dispozitivul să se încarce numai din spațiul de stocare local.

Vulnerabilitățile cunoscute sunt: porturile TCP/UDP deschise, porturile seriale deschise, mesajele de solicitare a parolelor de deschidere, locurile de inserare a codurilor, precum servere web, mesajele necriptate și conexiunile radio ar trebui să fie protejate. În cazul expedierilor, ambalajele rezistente la tampering îi vor permite destinatarului dispozitivului să afle dacă un dispozitiv a fost deschis înainte de sosire. Numărul și puterea protecției de la fiecare nivel depinde de tipul de amenințare, de nivelurile acceptabile de risc și de avantajele dorite (Rtherh et al., 2017).

2.2. Asigurarea de actualizări/corecții de firmware

Vulnerabilitățile vor fi descoperite, inevitabil, după implementarea dispozitivelor. Dispozitivele trebuie să permită corecții sau upgrade-uri. În mod normal, programele de tip firmware ale dispozitivelor ar trebui să poată fi modificate doar cu semnătura digitală adecvată. În situația actuală, furnizorii și producătorii de dispozitive nu au întotdeauna motivația financiară necesară pentru a asigura constant upgrade-uri de corecție IoT, deoarece veniturile lor provin în mare parte din vânzarea dispozitivului și nu din întreținerea acestuia. În aceste condiții, întreținerea dispozitivelor IoT poate să diminueze veniturile.

În plus, furnizorii nu sunt responsabili din punct de vedere legal pentru întreținerea continuă a dispozitivelor după vânzarea inițială, iar concurența îi determină pe furnizori să facă economii, diminuând calitatea în favoarea eficienței și a vitezei de lansare pe piață.

La fel de dăunătoare este preferința deliberată a furnizorilor pentru dispozitivele depășite (învechite), scopul fiind acela de a-și maximiza profiturile prin vânzări continue, mai degrabă decât prin întreținerea dispozitivelor existente. Mai mult, dispozitivele IoT nu sunt proiectate sau configurate în mod eficient pentru a răspunde la actualizările OTA (Over-the-Air), ceea ce presupune, în cel mai bun caz, niște proceduri costisitoare, iar în cel mai rău caz, proceduri imposibil de gestionat. În situația actuală, multe dispozitive IoT nu acceptă corecții și, ca atare, nu pot fi securizate. Cercetătorii au ajuns la concluzia că răspândirea generalizată a IoT și utilizarea unor dispozitive IoT nesecurizate și nesupravegheate în interiorul locuințelor și al companiilor va crește exponențial, deschizând noi oportunități pentru hackeri de a exploata vulnerabilitățile severe. Dincolo de faptul că sunt intenționat depășite, multe dispozitive IoT au un ciclu de viață limitat. Companiile trebuie să fie obligate să își asume responsabilitatea legală de a monitoriza și de a întreține dispozitivele de-a lungul unor cicluri de viață recomandate și stabilite de comun acord. În acest scop, trebuie să existe anumite standarde prestabilite și să fie instituită o legislație specifică. În plus, furnizorii trebuie să rămână transparenți și deschiși cu privire la ciclul de viață al dispozitivelor, în special în ceea ce privește politicile de servicii și întreținere, inclusiv în privința perioadei de timp pentru care intenționează să asigure asistența necesară pentru dispozitivele lor. Ei trebuie să își asume un rol activ în furnizarea de detalii privind corecțiile și upgrade-urile, ca și în privința preocupărilor legate de riscurile de securitate și confidențialitate, asigurându-se că respectivul consumator și/sau utilizator este informat în legătură cu modificările politicii, funcționalității și securității.

Trebuie luat în considerare ciclul de viață complet al dispozitivului IoT, începând de la momentul fabricației, când acreditările de securitate trebuie să fie „generate, alocate și incluse în dispozitive într-o manieră sigură”. De asemenea, informările trebuie să includă și ciclul de viață al producătorului original. După ce furnizorul original nu mai există, devine imposibilă identificarea sursei acreditărilor în vederea corectării vulnerabilităților și a breșelor de securitate, deoarece furnizorii sunt inevitabil înlocuiți și/sau ies de pe piață ori intră în faliment.

2.3. Realizarea de teste dinamice

Este esențial ca dispozitivele IoT să fie supuse unor teste amănunțite și să se stabilească un nivel minim de referință privind securitatea. Testele statice nu au fost concepute pentru descoperirea vulnerabilităților existente în componentele disponibile pe piață, precum procesoare sau memorie în care poate exista o componentă a aplicației generale. Testarea dinamică, pe de altă parte, poate scoate la iveală atât punctele slabe ale codului, cât și eventualele defecte sau vulnerabilități subiacente, provenite din hardware și care ar putea să nu fie vizibile la analiza statică. Testarea dinamică poate descoperi vulnerabilități care apar atunci când un cod nou este utilizat pe procesoare vechi. Recomandarea către producătorii care achiziționează hardware și software de la alți producători este de a face teste dinamice pentru a se asigura că produsele respective sunt sigure.

2.4. Specificarea procedurilor de protejare a datelor după eliminarea dispozitivelor

Odată cu trecerea timpului, dispozitivele se învechesc, iar utilizatorii ar putea decide să le arunce. Dispozitivele trebuie eliminate fără riscul de expunere a datelor confidențiale. Aceasta este o problemă de securitate, deoarece dispozitivele eliminate în mod necorespunzător ar putea fi convertite pentru a servi unor scopuri rău intenționate. Este, în același timp, o problemă de confidențialitate, deoarece, dacă este lăsat în funcțiune sau eliminat în mod necorespunzător, hardware-ul vechi ar putea fi utilizat pentru a dezvălui informații personale despre utilizator sau despre alți participanți direct interesați din ecosistemul IoT. Același lucru este valabil și în cazul dispozitivelor IoT vândute către un alt proprietar sau care devin echipamente standard în locuințe și sunt transmise mai departe odată cu vânzarea casei.

Ideal ar fi ca producătorii de produse IoT să pregătească un plan formal pentru ca utilizatorii să curețe și să arunce dispozitivele IoT vechi. Practica industrială din alte domenii recomandă o politică de „eliminare, reciclare sau distrugere” (discard, recycle or destroy - DRD), cu revizuirea

periodică a planului pentru a stabili ce dispozitive trebuie să fie eliminate și cum anume pot fi eliminate. Unii producători încurajează utilizatorii să elimine produsele apelând direct la producător. Această soluție s-ar putea dovedi practică în cazul laptopurilor și al serverelor, însă în cazul dispozitivelor IoT, care pot fi mici și ieftine sau care fac parte dintr-un dispozitiv mult mai mare (precum un frigider, de exemplu), ar putea fi necesare spații speciale.

La achiziționarea unui produs IoT la mâna a doua, utilizatorii individuali ar putea încerca să descopere ce informații de identificare personală (PII - Personally Identifiable Information) sau informații de autentificare (precum nume de utilizator și parolă - UNPW) rămân stocate pe dispozitiv, pot fi accesate de pe dispozitiv sau trebuie stocate în altă parte pentru a putea utiliza dispozitivul. Spre exemplu, Amazon Echo Dot le solicită utilizatorilor să stocheze parolele routerelor de rețea Wi-Fi pe un server Amazon. Se pune întrebarea dacă se așteaptă și de la utilizatori să stabilească sau nu o politică DRD individuală, care poate presupune ștergerea informațiilor dintr-o locație accesibilă pe Internet, alta decât dispozitivul în sine.

În situația actuală, utilizatorii nu dispun de o pregătire adecvată, pentru că nu posedă competențele digitale necesare pentru a se orienta la acest nivel de securitate și nu sunt suficient de bine echipați pentru a înțelege aspectele complexe ale stocării parolelor în dispozitivele conectate. Dezvăluirea acestor aspecte complexe vine adesea prea târziu, așa cum s-a întâmplat recent, când s-a aflat că faxurile și copiatoarele moderne au unități hard disk care păstrează copii ale documentelor. Nici utilizatorii din corporații, cu departamente IT instruite în domeniul securității, nu conștientizaseră acest lucru. Implicațiile pentru securitate din exemplul de mai sus sunt numeroase și arată cât este de simplu ca vicii majore de securitate să rămână nejustificate.

3. Bune practici privind securizarea rețelelor

3.1. Folosirea de metode de autentificare puternice

Dispozitivele IoT nu ar trebui să apeleze la folosirea numelor de utilizator și parolă ușor de intuit, precum admin/admin. Dispozitivele nu ar trebui să utilizeze acreditări implicite care sunt invariabile pe mai multe dispozitive și nu ar trebui să includă metode secrete de acces și setări ascunse ale modului de depanare (acreditări secrete stabilite de programatorul dispozitivului), deoarece, odată intuite, ele pot fi utilizate pentru a „sparge” (accesa) mai multe dispozitive.

Fiecare dispozitiv ar trebui să aibă propriile combinații implicite, unice, de nume de utilizator/parolă, eventual imprimate pe carcase și, de preferință, resetabile de către utilizator. Parolele ar trebui să fie suficient de complexe pentru a rezista în fața metodelor de deducție din aproape în aproape sau a celor care presupun forța brută. Acolo unde este posibil, recomandăm autentificarea cu doi factori (two-factor authentication - 2FA), prin care i se solicită unui utilizator să folosească simultan și o parolă, și o altă formă de autentificare care nu se bazează pe cunoștințele utilizatorului (de exemplu, un cod aleatoriu, generat prin SMS).

Pentru aplicațiile IoT, se recomandă în mod special autentificarea pe bază de context (Context-Aware Authentication – CAA), cunoscută și sub denumirea de „autentificare adaptivă”, în care informațiile contextuale și algoritmii de învățare programată/machine-learning evaluează constant riscul de atac malițios, fără a mai deranja utilizatorul prin solicitarea autentificării. Dacă riscul este mare, abonatului (sau hacker-ului) i se va cere un token multi-factor pentru a avea în continuare acces.

3.2. Folosirea de metode puternice de criptare și protocoale securizate

Chiar dacă parolele dispozitivelor sunt sigure, comunicările dintre dispozitive pot fi accesate neautorizat. În IoT există multe protocoale (de exemplu: Bluetooth, Zigbee, Z-Wave, 6LoWPAN, Thread, Wi-Fi, cellular, NFC, Sigfox, Neul și LoRaWAN), iar în funcție de protocol și de resursele de calcul disponibile, un dispozitiv poate fi mai mult sau mai puțin capabil să utilizeze o criptare puternică.

Producătorii ar trebui să facă o analiză de la caz la caz și să apeleze la cea mai puternică metodă de criptare posibilă, de preferință IPsec și/sau TLS/SSL. Pot exista situații în care criptarea nu este de dorit, ca în cazul SAE J2735 Basic Safety Messages (BSM) – comunicațiile wireless pe care le pot folosi mașinile pentru evitarea coliziunilor. În astfel de situații, mesajele pot fi transmise în mod deschis și pot fi verificate prin semnături digitale.

Cu toate acestea, nu trebuie neglijate implicațiile omiterii criptării. În cazul SAE J2735, mesajele de tip BSM pot fi folosite pentru a emite alerte false către sistemele de gestionare a coliziunilor și a imobiliza astfel un autovehicul. Nu există o soluție standard pentru a evita necesitatea unei echilibrări atente a tipurilor de amenințare anticipate și a vulnerabilităților care vor fi tolerate. Dacă datele sunt transmise necriptate și nesemnate, vor trebui luate măsuri de precauție pentru garantarea faptului că datele false au șanse minime spre inexistente de a provoca daune.

3.3. Reducerea la minimum a lățimii de bandă folosită de un dispozitiv

Recent, atacuri de tip DDoS (Distributed Denial-of-Service) au fost desfășurate folosind dispozitive IoT slab protejate, care s-au transformat în sisteme zombi în cadrul unor campanii masiv informatizate. Cele mai multe dispozitive IoT sunt fabricate din componente de larg consum care au capacități de rețea extrem de performante pentru funcția pe care ar trebui să o îndeplinească, provocând astfel încărcări ale rețelelor casnice și putând contribui la acumularea unor costuri imense în cazul atacurilor DDoS declanșate prin intermediul IoT.

Să presupunem că în viitor ar exista 50 de miliarde de dispozitive conectate la Internet, iar 1,1% dintre ele (calculând pe baza situației actuale) ar fi compromise și s-ar afla sub comandă coordonată de la distanță, însemnând 55 milioane de dispozitive IoT „rău intenționate”. Să presupunem că fiecare dispozitiv este capabil să genereze trafic de atac cu viteză echivalentă cu gigabit Ethernet (81.274 – 1.488.096 cadre pe secundă), de exemplu: soluția de tip system-on-a-chip (SoC) ARM9 are două astfel de conexiuni încorporate, iar fabricarea ei costă mai puțin de 5 USD pentru fiecare chip. Folosind această armată zombi de 55 de milioane de dispozitive pentru a genera evenimente DDoS, atacatorii ar putea genera între 4,47 și 81,8 trilioane de cadre pe secundă sau 55 petabiți pe secundă, depășind cu mult capacitățile de apărare ale unui singur furnizor de servicii. Un atac de o asemenea amploare ar putea distruge cea mai rapidă interfață de rețea construită până în momentul de față (300 Gbps) cu o marjă de 183.333 la 1.

Nu există o metodă potrivită pentru a reduce traficul „rău intenționat” generat de aceste sisteme, cu excepția eliminării lui de la sursă. Producătorii de dispozitive ar trebui să limiteze volumul de trafic de rețea pe care îl pot genera dispozitivele IoT până la niveluri rezonabile necesare pentru îndeplinirea funcțiilor specifice. Nu este necesar ca un frigider conectat la Internet să emită mesaje de tip Internet Control and Management Protocol (ICMP) la viteze de 1 gigabit pe secundă. Deși unele frigidere sunt echipate cu ecrane video, cel mai probabil ele nu au nevoie de capacități de încărcare de mare viteză.

Furnizorii ar trebui să aplice limitări ale lățimii de bandă la nivel de bază și hardware pentru a regla viteza de transmisie a rețelei la niveluri rezonabile pentru sarcinile fiecărui dispozitiv. Astfel de limitări fac ca unui atacator să îi fie mult mai greu să utilizeze un dispozitiv într-un atac DDoS, chiar dacă l-a compromis complet. În plus, dispozitivele ar trebui să fie programate pentru auto-monitorizarea comportamentelor neobișnuite și revenirea la setările din fabrică în situația în care este detectat un comportament alarmant.

Dacă revenirea dispozitivelor la setările din fabrică nu este posibilă, dispozitivele ar trebui cel puțin să poată să se reinițializeze pentru a șterge codul pe care atacatorul îl rulează în memoria lor. Acum, presupunând că cele 55 de milioane de dispozitive IoT „rău intenționate” menționate mai sus ar avea lățime de bandă atenuată impusă de hardware/nucleu, de exemplu, la 10 cadre Ethernet pe secundă, profilul lor potențial de atac agregat scade până la 550 de milioane de cadre pe secundă, respectiv nu mai mult de 6,6 terabiți pe secundă. Este o capacitate de 150.000 de ori mai mică și, chiar dacă este încă prea mare pentru un singur apărător, un atac de o asemenea anvergură poate fi oprit de un grup dispersat de apărători.

Controalele suplimentare la nivel de bază din dispozitive, care observă și atenuează volumele mari de trafic încărcat sau opresc alte comportamente neașteptate, ar putea diminua și mai mult capacitățile distructive ale dispozitivelor compromise, fără a necesita eforturi prea mari din partea administratorilor de rețea. Astfel, se recomandă o analiză serioasă a cerințelor de performanță ale fiecărui dispozitiv și implementarea unor limitări acceptabile. Acest lucru va îmbunătăți considerabil siguranța dispozitivelor IoT și va face posibilă introducerea și folosirea în siguranță a multor asemenea dispozitive în viitor.

3.4. Segmentarea rețelelor

Segmentarea rețelei în rețele locale mai mici folosind Virtual Local Area Network VLAN-uri, range-uri de adrese IP sau o combinație între acestea va îmbunătăți considerabil siguranța dispozitivelor IoT. Segmentările de rețea sunt utilizate în politici de securitate tip Next-generation firewall pentru a identifica în mod clar una sau mai multe interfețe sursă și destinație pe echipament. Fiecare interfață a unui firewall trebuie să fie alocată unei zone de securitate înainte de a putea procesa traficul. Acest lucru le permite organizațiilor să creeze zone de securitate care să reprezinte diferite segmente conectate la firewall și controlate de acesta. De exemplu, administratorii de securitate pot aloca toate depozitele de date ale deținătorilor de carduri sau ale pacienților într-un singur segment de rețea identificat printr-o zonă de securitate (de exemplu, „Date despre clienți”). Apoi, administratorul poate elabora politici de securitate care să le permită doar anumitor utilizatori, grupuri de utilizatori, aplicații sau altor zone de securitate să acceseze zona „Date despre clienți”, împiedicând astfel accesul intern sau extern neautorizat la datele stocate pe respectivul segment.

Acest tip de soluție este mai frecvent întâlnit în aplicațiile industriale, dar poate fi utilă și în circumstanțe mai extinse. O rețea privată separată, detașată, pentru un sistem de securitate, poate cu un canal dedicat unei baze centrale de operațiuni, în cazul unui sistem de securitate casnic, ar putea fi un exemplu bun. Dacă sistemul trebuie să folosească Internetul, ar putea fi implementată o rețea privată virtuală (VPN).

4. Bune practici privind securizarea globală a sistemelor IoT

4.1. Protejarea informațiilor sensibile

Principiul de bază al IoT este acela de a conecta obiectele de uz curent prin Internet sau o rețea ad-hoc. Dispozitivele IoT oferă servicii care pot fi descoperite de alte dispozitive IoT. Majoritatea protocoalelor „scurg” informații sensibile de identificare personală (PII - Personally Identifiable Information), precum numele proprietarului ori alte informații care pot fi asociate cu o persoană, de exemplu, numele gazdei unui dispozitiv. Aceste informații pot fi legate de alte surse de informații pentru a dirija atacurile. Sunt necesare mecanisme de protecție și protocoale de autentificare, astfel încât numai clienții autorizați să poată descoperi dispozitivul.

4.2. Încurajarea hacking-ului etic și descurajarea garanțiilor blanket safe harbor

Recent a fost elaborat un proiect de lege pentru Senatul Statului Michigan care propune pedepsirea hacking-ului printr-o condamnare la închisoare pe viață. Unul dintre autorii proiectului l-a contactat pe unul dintre senatorii care au propus legea, iar respectivul senator a fost de acord să modifice proiectul în așa fel încât hacking-ul să fie permis în scopuri benefice de cercetare (de exemplu: cercetătorii care descoperă vulnerabilități grave pe care le raportează în mod responsabil făcând un serviciu industriei, la fel ca și aceia care descoperă erori de securitate la automobile și alte utilaje în cazul cărora siguranța este crucială). Cercetările legitime în domeniul securității pot fi îngreunate de legislația excesivă. O metodă de a face diferența între cercetare și hacking-ul neetic este aceea de a impune divulgarea responsabilă a vulnerabilităților descoperite. Divulgarea responsabilă presupune ca cercetătorul să informeze mai întâi producătorul sau autoritățile și să acorde un răgaz rezonabil pentru ca vulnerabilitatea respectivă să fie verificată și remediată independent înainte de a face public vulnerabilitatea de sistem. O altă abordare, mai puțin dezirabilă, ar putea fi aceea de a le cere cercetătorilor să se înregistreze mai întâi la un birou guvernamental sau la producător înainte de a încerca să pătrundă într-un dispozitiv.

Fără îndoială, legislația ar trebui să promoveze un ecosistem IoT sigur și util pentru toți. Legislația ar trebui să îi pedepsească pe infractori. Însă, în egală măsură, legislația ar trebui să evite scoaterea în afara legii a acelor activități care ajută la promovarea siguranței și securității. Legislația ar trebui să evite să acorde protecție legală activităților care creează prejudicii. Această poziție a fost exprimată cât se poate de clar de Terrell McSweeny, membră a Comisiei Federale pentru Comerț (FTC – Federal Trade Commission), în cadrul conferinței Connected Cars – SUA 2016.

Producătorii nu beneficiază financiar de pe urma expunerii defectelor din produsele lor, dar aceste defecte trebuie să fie identificate pentru îmbunătățirea funcționalității și securității. Programele de recompense pentru raportarea bug-urilor (programe plătite de producători) îi pot ajuta pe aceștia din urmă să atenueze publicitatea negativă din presă, îmbunătățind totodată calitatea produselor la un cost mai mic decât costul angajării unor specialiști în teste de penetrare plătiți. Autoritățile legislative ar trebui să ia măsuri de precauție pentru a împiedica acțiunile în instanță împotriva hackerilor etici. Legislația ar trebui să cuprindă prevederi explicite care să permită cercetarea și hacking-ul etic. În același timp, ar trebui să fie evitate clauzele de protecție legală a producătorilor care ar putea implementa produse nesigure, dăunătoare, în scopul unor câștiguri financiare. Producătorii, utilizatorii/cetățenii și în special inginerii/cercetătorii ar trebui să fie în permanență informați în legătură cu legile aflate în curs de promulgare și să le comunice legiuitorilor pozițiile lor.

4.3. Instituirea unei Comisii de Certificare pentru Securitate și Confidențialitate IoT

Din cauza problemelor frecvente de securitate și confidențialitate provocate de dispozitivele IoT, inginerii trebuie să își asume responsabilitatea pentru propriile creații. IEEE (Institute of Electrical and Electronics Engineers) sau oricare altă organizație internațională ar trebui să asigure un program de certificare profesională pentru creatorii, constructorii și furnizorii noilor tehnologii IoT care se angajează să respecte cele mai bune practici instituite pentru crearea de noi dispozitive IoT. Comisia de validare a programelor ar trebui să fie autorizată să verifice dacă furnizorul respectă practicile de inginerie responsabilă (în special acele practici care fac posibile securitatea și confidențialitatea IoT) și dacă îi susține pe furnizorii obligați să respecte aceste practici. Acțiunile negative ar fi o altă dimensiune a acestui program de certificare și ar trebui să fie limitate la pierderea statutului de certificare și eventual la raportarea către FTC sau o altă autoritate guvernamentală în vederea unor acțiuni ulterioare.

Organismul de certificare ar trebui să verifice cel puțin următoarele elemente ale produselor, protocoalelor și documentelor unui furnizor:

- datele sunt gestionate, utilizate, protejate și partajate în mod responsabil;
- protocoalele utilizate sau recomandate nu scurg informații despre utilizatori, dincolo de intenția explicită a acestor utilizatori;
- când apar probleme de confidențialitate, furnizorul certificat răspunde prompt despre acestea;
- metodele de autentificare sunt suficient de puternice și respectă protocoalele dovedite;
- dispozitivele nu sunt supraalimentate sau insuficient protejate;
- dispozitivele ar trebui să aibă o etichetă de identificare care să nu poată fi falsificată cu ușurință și care să conțină un link web pe care clienții să-l poată accesa pentru a afla starea de certificare a dispozitivului, împreună cu o descriere a acestuia (model și număr de serie etc.). Acest lucru poate fi făcut în colaborare cu FTC sau alte organisme naționale.

Astfel de programe de certificare reduc gradul de incertitudine și le oferă producătorilor de dispozitive, inginerilor și autorilor cele mai bune practici de urmat. Instanțele pot considera certificarea o dovadă a faptului că există practici acceptabile, care sunt, în general, respectate. În eventualitatea unor litigii, un furnizor poate indica certificarea, spunând că a respectat bunele

practici de inginerie (Rtherh et al., 2017; Technical working group report, a broadband internet technical advisory group, 2016).

5. Instrumente software de securitate IoT

Securitatea Internet of Things sau securitatea IoT implică soluții pentru protejarea dispozitivelor inteligente și a hub-urilor IoT centralizate împotriva accesului sau manipulării nedorite. Tehnologiile de securitate IoT se extind și evoluează pentru a satisface cerințele de securitate cibernetică și IoT în ansamblu. Produsele din această categorie au aceleași caracteristici de bază ale altor tipuri de software de securitate IT și sunt construite pentru a se integra cu instrumentele de management IoT, pentru a oferi companiilor o utilizare completă și fiabilă a acestei rețele.

5.1. SeaCat.io

Este o tehnologie de securitate de tip Software as a Service - SaaS care administrează și operează produsele IoT într-o manieră fiabilă, scalabilă și sigură. Oferă protecție utilizatorilor finali, afacerilor și datelor. Principalele caracteristici ale acestui produs (SeaCat - Cyber-security and data privacy platform for mobile and IoT applications, 2020) sunt:

- gestionarea echipamentelor IoT dintr-o consolă centrală (Figura 1);
- accesarea dispozitivelor de la distanță folosind diverse instrumente;
- monitorizarea flotei de dispozitive conectate folosind tablouri de bord intuitive;
- automatizarea actualizărilor pentru remedierea erorilor, lansare de noi funcții sau securizare rapidă;
- protejarea utilizatorilor folosind tehnici criptografice autorizate respectând reglementări în vigoare;
- opțiunea VPN SSL pentru toate dispozitivele, inclusiv reînnoirea certificatelor automate;
- detecția de malware și asigurarea că dispozitivele IoT nu conțin programe malițioase;
- notificare - astfel încât să nu se piardă nimic prin serviciul de alertă automată; redirecționarea oricărui incident în mod proactiv; detectarea posibilelor încercări de intruziune sau a perioadelor de nefuncționare;
- integrarea cu SIEM-ul, cu sistemul de management al identității, cu jurnalele de loguri, cu sistemele de detectare a intruziunilor și multe altele;
- protocoalele suportate: HTTP, MQTT, SSH, VNC, TCP/IP, Syslog, LDAP, CEF etc.

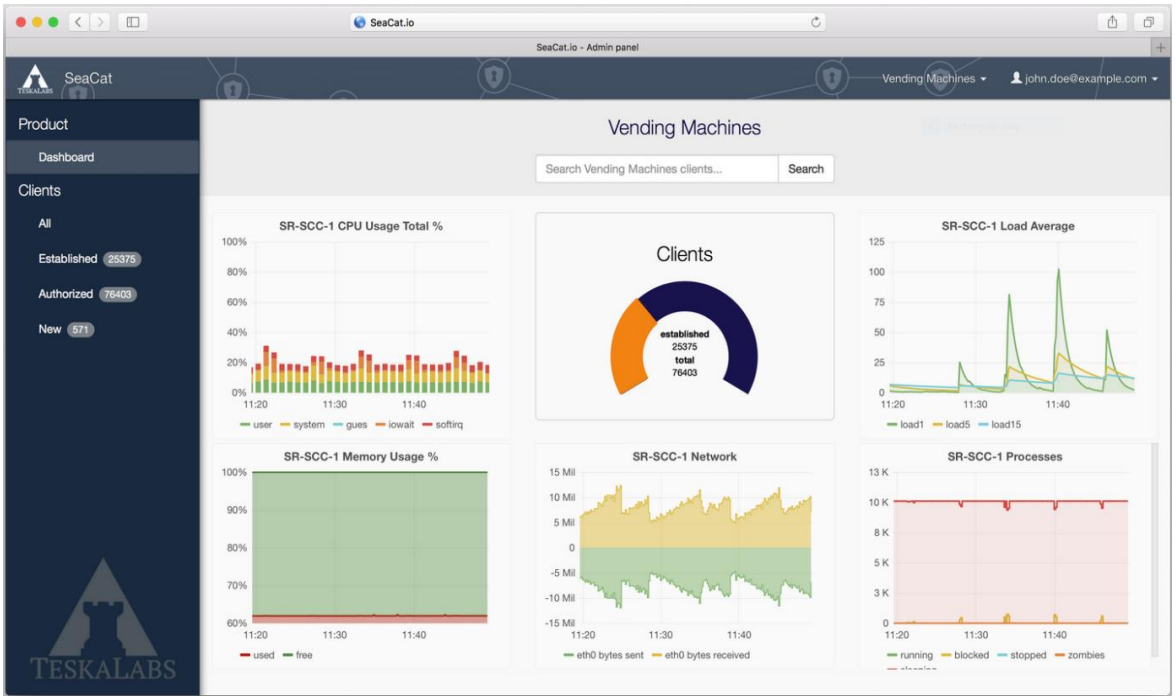

Figura 1. SeaCat.io – Panoul de administrare (SeaCat Powerfull Dashboards, 2020)

(Sursa: https://teskalabscom.azureedge.net/media/screenshots/seacat-io-dashboard-full.png)

5.2. Digicert Home and Consumer IoT Solution

Protejează datele private și comunicația dintre dispozitivele IoT prin prevenirea accesului neautorizat folosind Infrastructura cheii publice (PKI). DigiCert Cloud PKITM este o platformă ce permite implementarea și gestionarea a milioane de certificate IoT, previzionarea, emiterea, reînnoirea și revocarea certificatelor făcându-se dintr-un panou unic de administrare (Home and Consumer IoT Security Solutions, 2020).

5.3. Zvelo IoT Security

Este oferta de securitate IoT a producătorului de tehnologii Zvelo și se axează pe dezvoltarea de servicii de detecție și catalogare bazate pe inteligență artificială (AI - Artificial intelligence), pentru a oferi cele mai exacte și mai complete profiluri și detecții de anomalii pentru produsele IoT și dispozitivele conectate la web. Zvelo IoT Security este o soluție concepută pentru a integra mai multe tipuri de echipamente precum routere wireless, routere gateway sau dispozitive UTM (Unified Threat Management) și acceptă rețele WiFi, Bluetooth, LoRa și de bandă îngustă.

În centrul platformei de securitate IoT de la Zvelo se află „zENSOR” un senzor software ce are la baza algoritmi ce permit o descoperire dinamică a dispozitivelor, catalogarea completă a dispozitivelor, precum și detectarea dispozitivelor compromise. Soluția poate recunoaște fără nici o informație în prealabil dispozitivele IoT și BYOD (Bring Your Own Device) dintr-o rețea, pe care apoi le monitorizează continuu cu scopul de a determina dacă comportamentul indică compromiterea acestuia folosind amprentele comportamentale unice (MAC, OS, agenți) și tiparele de trafic (interogări DNS, apeluri API), precum și inteligența artificială.

Fiecare dispozitiv primește un scor („zSCORE”) bazat pe încredere, potențial de vulnerabilitate și reputație. Acest scor este actualizat continuu pe măsură ce sunt observate noi date și evenimente (IoT Security Technology For Router & Gateway Manufacturers, 2020).

5.4. KeyScaler

Device Authority este un lider global în managementul identității (Identity and Access Management - IAM) pentru IoT și Blockchain. Platforma KeyScaler™ oferă încredere atât dispozitivelor IoT cât și ecosistemului IoT, pentru a aborda provocările securizării IoT. KeyScaler™ folosește o tehnologie avansată, inclusiv Dynamic Device Key Generation (DDKG) și PKI (Public Key Infrastructure) Signature+, care oferă simplitate și încredere dispozitivelor IoT, permițând clienților să se înregistreze în siguranță, să furnizeze și să conecteze dispozitive la platforme, aplicații și servicii IoT. Platforma simplifică procesul de stabilire a unei arhitecturi de securitate robuste, end-to-end în cadrul IoT și oferă eficiența prin automatizarea securității, fără intervenția umană (Introducing KeyScaler as as Service - IoT security, IAM, managed in the cloud, 2020).

5.5. Azure IoT

Este o platforma care conectează, monitorizează și controlează miliarde de active IoT. De asemenea, include sisteme de securitate și de operare pentru dispozitive și echipamente, împreună cu date și analize care ajută companiile să construiască, să implementeze și să gestioneze aplicații IoT (Explore the benefits of Azure IoT, 2020).

5.6. Cloud IoT Core

Google Cloud Internet of Things (IoT) Core este un serviciu complet privind gestionarea în siguranță a dispozitivelor IoT. Stochează date de la milioanele de dispozitive conectate și construiește diverse aplicații care se integrează cu celelalte servicii Big Data din platforma de Cloud Google. Datele de telemetrie ale dispozitivului sunt redirecționate către obiectul Cloud Pub/Sub, care poate fi apoi utilizat pentru a declanșa funcțiile Cloud. De asemenea, se pot efectua analize în timp real (streaming) cu Cloud Dataflow sau analize personalizate (Cloud IoT Core overview, 2020).

5.7. Expander

Este un instrument realizat de către Expanse și detectează sistemele și serviciile, care aparțin unei organizații, publicate în internet, furnizând informații utile, specializate care vizează perechea port-protocol. Combinând aceste informații cu o serie de seturi de date publice, instrumentul este capabil să detecteze complet și corect sistemele și servicii publicate în internet aparținând unei organizații. Pe lângă descoperirea echipamentelor aflate în infrastructura proprie, Expanse găsește și obiectele care aparțin organizației de la toți furnizorii de cloud - precum AWS (Amazon Web Services), Azure și GCP (Google Cloud Platform) (Expander – A Better Way to Manage Your Attack Surface, 2020).

Alte produse software de securitate folosite în IoT sunt:

- Pulse: IoT Security Platform - https://www.pwnieexpress.com;
- Symantec IoT Security - https://www.symantec.com;
- Darktarce - https://www.darktrace.com;
- Cisco IoT Threat Defense - https://www.cisco.com;
- Cisco Umbrella - https://umbrella.cisco.com;
- Net-Shield - https://github.com;
- Noddos - https://www.noddos.io;
- AWS IoT Device Defender - https://aws.amazon.com;
- Bayshore Industrial Cyber Protection Platform - https://www.bayshorenetworks.com;

- Trustwave Endpoint Protection Suite - https://www.trustwave.com;
- NSFOCUS ADS - https://nsfocusglobal.com;
- Norton Core - https://us.norton.com;
- Carwall - https://karambasecurity.com;
- SecBee - https://github.com;
- Bullguard IoT Scanner - https://IoTscanner.bullguard.com;
- Mirai Vulnerability Scanner - https://www.incapsula.com;
- Kaspersky IoT Scanner - https://play.google.com.

6. Concluzii

Securitatea cibernetică este importantă, deoarece cuprinde protejarea datelor noastre sensibile, a informațiilor de identificare personală, a informațiilor de sănătate, a proprietății intelectuale, a datelor și a sistemelor de informații guvernamentale și industriale împotriva furtului. Atacurile cibernetice sunt în ziua de azi frecvente iar rapoartele recente arată că hackerii atacă un computer în SUA la fiecare 39 de secunde.

La momentul actual, atacurile cibernetice și spionajul digital reprezintă cea mai mare amenințare la adresa securității naționale a unei țări.

De aceea este important să încercăm să prevenim aceste atacuri înainte ca ele să provoace daune importante, pierderi materiale și de date. Prevenirea acestor atacuri se poate face prin soluții de urmărire a unor indicatori. Prin monitorizarea acestor indicatori ne putem da seama dacă se întâmplă ceva ieșit din comportamentul normal al dispozitivelor și se pot lua măsuri preventive pentru evitarea unor întreruperi în funcționarea echipamentelor, pentru evitarea unor pierderi de date care pot duce chiar și la pierderi financiare însemnate.

Prevalența dispozitivelor IoT nesigure pe Internet face foarte probabil ca, în viitorul previzibil, acestea să fie principala sursă de atacuri de tip Distributed Denial-of-Service.

Confirmare

Acest articol a fost realizat în cadrul Proiectului *„Studiu privind securitatea comunicațiilor de date în medii smart”* finanțat de Planul sectorial al Ministerului Comunicațiilor și Societății Informaționale (MCSI), Contract 64/30.05.2018. Mulțumim colegilor din proiect pentru colaborare.

BIBLIOGRAFIE

1. Banciu, D., Rădoi, M., Belloiu, Ș. (2020). *Information Security Awareness in Romanian Public Administration: An Exploratory Case Study*. Studies in Informatics and Control, ISSN 1220-1766, vol. 29(1), 121-129, 2020.
2. Cîrnu, C. E., Rotună, C. I., Vevera, A. V., Boncea, R. (2018). *Measures to Mitigate Cybersecurity Risks and Vulnerabilities in Service-Oriented Architecture*. Studies in Informatics and Control, ISSN 1220-1766, vol. 27(3), 359-368, 2018.
3. *** *Cloud IoT Core overview*, disponibil la adresa: https://cloud.google.com/iot/docs/concepts/overview, accesat noiembrie 2020.
4. *** *Expander – A Better Way to Manage Your Attack Surface*, disponibil la adresa: https://expanse.co/wp-content/uploads/2020/10/Expanse-Expander-Datasheet.pdf, accesat noiembrie 2020.

5. *** *Explore the benefits of Azure IoT*, disponibil la adresa: https://azure.microsoft.com/en-us/overview/iot/, accesat noiembrie 2020.
6. *** *Home and Consumer IoT Security Solutions*, disponibil la adresa: https://www.digicert.com/internet-of-things/home-and-consumer/, accesat noiembrie 2020.
7. *** *IoT Security Technology For Router & Gateway Manufacturers*, disponibil la adresa: https://zvelo.com/industries/iot-security/, accesat noiembrie 2020.
8. *** *Introducing KeyScaler as as Service - IoT security, IAM, managed in the cloud*, disponibil la adresa: https://www.deviceauthority.com/video/introducing-keyscaler-service-iot-security-iam-managed-cloud, accesat noiembrie 2020.
9. Rtherh, G. C., Fink, G., Aledhari, A., Bielby, J., Nighot, R., Mandal, S., Aneja, N., Hrivnak, C., Cristache, L. (2017). *Internet of Things (IoT) Security Best Practices*, disponibil la adresa: https://internetinitiative.ieee.org/images/files/resources/white_papers/internet_of_things_feb2017.pdf, accesat noiembrie 2020.
10. *** *SeaCat - Cyber-security and data privacy platform for mobile and IoT applications*, disponibil la adresa: https://teskalabs.com/products/seacat, accesat noiembrie 2020.
11. *** *SeaCat Powerfull Dashboards*, disponibil la adresa: https://teskalabscom.azureedge.net/media/screenshots/seacat-io-dashboard-full.png, accesat noiembrie 2020.
12. *Technical working group report, a broadband internet technical advisory group (2016)*: Internet of Things (IoT) Security and Privacy Recommendations, disponibil la adresa: https://www.bitag.org/documents/BITAG_Report_-_Internet_of_Things_(IoT)_Security_and_Privacy_Recommendations.pdf, accesat noiembrie 2020.
13. *The OWASP IoT Security Team*, 2018: disponibil la adresa: https://owasp.org/www-pdf-archive/OWASP-IoT-Top-10-2018-final.pdf, accesat noiembrie 2020.

Mihail DUMITRACHE este absolvent al Facultății de Electrotehnică, Universitatea Politehnica din București, specializarea „Inginerie Asistată de Calculator”, inginer și doctor în Inginerie Electrică. Deține studii masterale în specializarea „Inginerie Electrică”, Universitatea Politehnică din București și în specializarea „Administrație Publică Electronică”, Universitatea din București. Și-a început activitatea profesională în cadrul Institutului Național de Cercetare-Dezvoltare în Informatică – ICI București în anul 2002, ca programator. În prezent este Cercetător Științific gradul III, Șef la Departamentul „Administrare domenii RoTLD” și Lector Universitar la Universitatea din București. Este autor și coautor al unor studii și articole de specialitate.

Mihail DUMITRACHE PhD graduated from Politehnica University of Bucharest, Faculty of Electrical Engineering, with an Engineer’s Degree and, later on, a PhD in Computer Assisted Engineering. In between, he obtained two Master’s Degrees, one in Electrical Engineering, at “Politehnica” University of Bucharest and one in Electronic Public Administration, at Bucharest University. His professional career started at the National Institute for Research and Development in Informatics – ICI Bucharest in 2002 as a computer programmer. Currently, he is Scientific

Researcher grade III and Head of the .ro Domain Administration Department (RoTLD), and also Lecturer at the University of Bucharest. He is author and co-author of several scientific studies and articles.

Ionuț-Eugen SANDU este licențiat în Știința Sistemelor și a Calculatoarelor (2006), obține master în Administrație Publică Electronică în anul 2007. Din anul 2010 devine cercetător științific în cadrul Departamentului de Administrare Domenii .ro din cadrul Institutului Național de Cercetare-Dezvoltare în Informatică – ICI București, iar începând cu anul 2015 devine Șef Serviciu Tehnic RoTLD și Cercetător Științific gradul III în cadrul aceluiași Institut. Domeniile sale principale de interes sunt: administrare sisteme, dezvoltare de noi servicii, dezvoltare și mentenanță a infrastructurii de comunicații, precum și relația cu partenerii. În prezent este Director Tehnic al Institutului Național de Cercetare-Dezvoltare în Informatică – ICI București.

Ionuț-Eugen SANDU graduated university with a BS în Computer and Systems' Science (2006) and obtained a Master's Degree in Electronic Public Administration in 2007. In 2010, he became Scientific Researcher within the .ro Domain Administration Department (RoTLD) of the National Institute for Research and Development in Informatics - ICI Bucharest, and since 2015 is Scientific Researcher grade III and Head of the Technical Division of RoTLD, with responsibilities in systems' administration, development of new services, development and maintenance of communication infrastructures. He is also in charge with maintaining a close relationship with RoTLD's Partners. Currently, he is Technical Director of National Institute for Research & Development in Informatics – ICI Bucharest.

Ionuț PETRE a absolvit Facultatea de Electronică, Telecomunicații și Tehnologia Informației, Universitatea Politehnica din București în anul 2005. Este doctorand la Universitatea „Lucian Blaga" din Sibiu, Facultatea de Management. În prezent este cercetător la Institutul Național de Cercetare-Dezvoltare în Informatică – ICI București. Domeniile sale principale de interes sunt: Internetul obiectelor (IoT), e-Guvernare, Big Data, transformare digitală, guvernanță digitală, inginerie software, testare automată, biblioteci digitale.

Ionuț PETRE graduated the Faculty of Electronics, Telecommunications and Information Technology in 2005. He is a PhD student at University "Lucian Blaga" from Sibiu, Faculty of Management. Currently he works as Researcher at National Institute for Research and Development in Informatics – ICI Bucharest. His main areas of interest are: Internet of Things, e-Government, Big Data, digital transformation, digital governance, software engineering, automated testing, digital libraries.