Starptautiskā darba grupa datu aizsardzības un telekomunikācijas jautājumos

675.55.8

Darba dokuments
Lietu interneta (Internet of Things jeb IoT – angļu val.) **vadības sistēmu (firmware) programmatūras atjauninājumi**
62. tikšanās, 2017. gada 27. un 28. novembrī, Parīze (Francija)

Ievads

Aplēses attiecībā uz tiešsaistē esošo lietu interneta (LI) ierīču skaitu līdz 2020. gadam būtiski atšķiras. Tiek minēti gan 26 miljardi[1], gan 50 miljardi[2]. Neraugoties uz to, kurš skaitlis būs pareizais, internetam pieslēgtu ierīču skaits nākamo pāris gadu laikā būtiski palielināsies.

Terminam "lietu internets" nav vienotas definīcijas. Viens avots[3] definē LI kā "*globālu infrastruktūru informācijas sabiedrībai, kas sniedz piekļuvi moderniem pakalpojumiem, savienojot (fiziski un virtuāli) lietas, izmantojot esošās un topošās savstarpēji savietojamās informācijas un komunikāciju tehnoloģijas*". Vietne Internet Society interpretē lietu internetu plašākā nozīmē kā "*tīkla savienojamību un skaitļošanas iespējas ar objektiem, ierīcēm, sensoriem un lietām, kas ierasti netiek uzskatītas par datoriem*".[4]

Ierīču, kas izmanto LI, būtiskākā īpašība ir to savienojamība ar tīklu un spēja apkopot un nodot datus internetā pa vadu un bezvadu savienojumiem. Šo ierīču pieslēgums internetam sniedz dažādas priekšrocības, piemēram, attālinātu kontroli, attālinātas

[1] Vietne Gartner apgalvo, ka lietu internetam pieslēgto ierīču skaits līdz 2020. gadam sasniegs 26 miljardus. Gartner 2013. gada 12. decembra relīze pieejama:http://www.gartner.com/newsroom/id/2636073

[2] *Lietu internets: kā interneta nākamā evolūcija maina pilnīgi visu (The Internet of Things: How the Next Evolution of the Internet Is Changing Everything), 2011. gada aprīļa Cisco Baltā grāmata, pieejama:* http://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

[3] Vietnes Internet of things pārskats, ITU Telekomunikācijas standartizācijas sektora ieteikumihttp://www.itu.int/ITU-T/recommendations/rec.aspx?rec=y.2060

[4] Lietu internets: Vietne Internet Society, Pārskats, 2015., https://www.internetsociety.org/sites/default/files/ISOC-IoT-Overview-20151221-en.pdf

Secretariat
Berliner Beauftragte für
Datenschutz und Informationsfreiheit
Friedrichstr. 219
D-10969 Berlīne
Tālrunis +49 / 30 / 13889 0
Fakss: +49 / 30 / 215 5050

E-pasts:
IWGDPT@datenschutz-berlin.de
Tīmekļa vietne:
http://www.berlin-privacy-group.org

uztveršanas un automatizācijas iespējas, taču tas paaugstina risku, ka šīs ierīces un to apstrādātā informācija var tikt apdraudēta.
LI ekosistēma ir plaša un ietver dažādas nozares, tajā skaitā, bet ne tikai IT un interneta tīklus, drošību un publisko drošību, mazumtirdzniecību, transportu, rūpniecību, veselības aprūpi, patēriņa un mājokļa preces, enerģētiku, ēkas utt. LI ierīces parasti sastāv no vai ietver vienu vai vairākas vadības sistēmas (atsevišķus skaitļošanas moduļus), kuriem katram parasti ir viens noteikts apstrādes mērķis un kas kopā nodrošina nepieciešamo LI ierīces funkcionalitāti. Šādām vadības sistēmām ir ierobežots centrālais procesors, atmiņa un jaudas resursi (tā sauktās ierobežotās ierīces) ar "*īpašiem ierobežojumiem, tajā skaitā izmaksu, izmēra, svara un citiem ar apjomu saistītiem faktoriem*".[5] Šie ierobežojumi bieži nozīmē to, ka ražotāji savās ierīcēs neietver programmatūras/aparātprogrammatūras atjauninājumu mehānismu. LI ierīču piemēri ietver pieslēgtus vides sensorus (temperatūra, mitrums un spiediens), spuldzes, printerus un kameras mājokļa drošības sistēmā.
LI ierīču ražotāji parasti cenšas savos produktos izmantot, trešo pušu piegādātāju izstrādātas vadības sistēmas. Šo komponenšu pārdevēji var saražot miljoniem iegulto sistēmu gadā, un jebkuras izmaiņas šajā piegādes ķēdē aizņem daudz laika un ir dārgas. Saistībā ar laikietilpīgo piegādes ķēdes raksturu atsevišķas programmatūras komponentes var būt vairākus mēnešus vai gadus vecas, pirms tās tiek izmantotas gala produktā.
LI ierīču klātbūtnes dēļ tajās ietverto sensoru dažādība un to tuvums cilvēkiem, tajā skaitā iespēja implantēt tos cilvēka ķermenī var būtiski paaugstināt iespējamību, ka šīs ierīces apstrādās (apkopos, manipulēs, uzglabās, nodos) informāciju par visiem personas dzīves aspektiem (piemēram, fizioloģiskiem, uzvedības, atrašanās vietas utt.). Ņemot vērā, ka daudzas no šīm ierīcēm sazinās ierīču līmenī, apejot saziņu ar cilvēkiem, tās var radīt būtiskus riskus un apdraudēt personu pamattiesības un brīvības.
Šajā darba dokumentā apskatīti riski, kas saistīti ar nespēju atjaunināt aparātprogrammatūru, kas nodrošina LI ierīces darbību. Tāpat dokumentā apskatīti daži veiksmīgas atjaunināšanas aspekti (piemēram, jaunu iespēju ieviešana, kas personai nav zināmas). Šie riski ietver neatļautu ierīces iegūtu personas datu apkopošanas, mainīšanas vai atklāšanas risku, kā arī ierīces ievainojamību izmantošanu, izmantojot ierīci kā rīku, lai apdraudētu citu sistēmu integritāti, apstrādājot vai aizsargājot personas datus. Tādas ierīces kā personālie datori, planšetdatori, viedtālruņi, viedie TV, izklaides sistēmas pieslēgtos transportlīdzekļos utt. šajā dokumentā netiek apskatītas.

Kas ir aparātprogrammatūra?
Ierīces vadības sistēmas parasti ietver vienu vai vairākus mikrokontrollerus ar ierobežotu atmiņas un apstrādes spēju. Uz mikrokontrollera uzstādītā programmatūra ir īpaši paredzēta miktrokontrollera specifikācijām un noteiktam mērķim. Šo programmatūras veidu parasti sauc par aparātprogrammatūru, un tā nodrošina nepieciešamās norādes, kā ierīce sazinās ar citu datortehniku vai plašāku tīklu. Aparātprogrammatūra atrodas energoneatkarīgā atmiņā (zibatmiņā vai lasāmatmiņā (ROM)).

[5] Ierobežotu mezglu tīklu terminoloģija https://tools.ietf.org/html/rfc7228

Kāpēc aparātprogrammatūrai nepieciešama atjaunināšana?

Visu veidu programmatūra, pat tāda, kas daudz testēta, var saturēt kļūdas. Dažas no tām ražotājam ir zināmas, taču netiek labotas, lai ievērotu ražošanas termiņu, savukārt citas var kļūt zināmas pēc tam, kad ierīce ir nosūtīta. Šīs kļūdas atšķiras pēc to nozīmīguma. Dažas ir nebūtiskas un nerada būtisku ietekmi uz ierīces normālu darbību. Citas savukārt ir nozīmīgas un var izraisīt ierīces nenormālu uzvedību. Tāpat kā jebkuras programmatūras gadījumā ir vairāki iemesli, kāpēc aparātprogrammatūrai nepieciešama atjaunināšana:

a) lai pievienotu jaunas **funkcijas**;
b) lai **veiktu rekonfigurāciju,** balstoties uz mainīgiem interneta protokoliem;
c) lai izlabotu aparātprogrammatūras **kļūdas**; vai
d) lai aizvietotu **vājus kriptogrāfiskus algoritmus** vai **atslēgas** (visiem kriptogrāfiskajiem algoritmiem ir derīguma termiņš).

Kļūdas, kas ļauj uzbrucējam apdraudēt ierīces drošību[6] (t.i., programmatūras ievainojamība), var radīt apdraudējumu plašākam tīklam, kā arī datiem, ko ierīce apstrādā, un personai(-ām), uz kuru(-ām) dati attiecas.

Kā aparātprogrammatūru iespējams atjaunināt?

Aparātprogrammatūras savlaicīga un pareiza atjaunināšana ir pietiekami sarežģīta ar tradicionālajām skaitļošanas ierīcēm. Iezīmes, kas definē iegultās sistēmas LI ierīcēs, ietver šos sarežģījumus un rada jaunus.

Iegultajām sistēmām bieži trūkst veidu, kā piedāvāt personai vienkāršu vai automātisku aparātprogrammatūras atjaunināšanas procesu, kas var tikt izmantots, kad ierīce atstāj ražotāju. Tas saistīts ar vairākiem faktoriem, tajā skaitā ierīces specifikāciju vai dizainu. Aparātprogrammatūras atjauninājumi, ja ražotājs tos piedāvā, parasti pieejami atbalsta vietnē, kur persona tos var lejupielādēt un manuāli uzstādīt. Manuāla uzstādīšana bieži sākas ar aparātprogrammatūras uzbūves (arhitektūras) apraksta nodošanu, izmantojot standarta vai izstrādātāja protokolu, kas spēj vai nespēj autentificēt personas, kas ir pilnvarotas sākt šo procesu. Tam nepieciešama aparātprogrammatūras uzbūves (arhitektūras) apraksta nodošana LI ierīcei, iespējams, pieslēdzoties ierīcē iebūvētajam tīmekļa serverim, pieslēdzot USB ierīcei vai izmantojot citu metodi. Ievērojiet, ka dažām LI ierīcēm nav tradicionālās lietotāja saskarnes vai nav lietotāja saskarnes vispār. Atjauninājuma piemērošana var būt tikpat vienkārša, cik failu arhīva atvēršana, taču tam var būt nepieciešama arī ierīces pārlikšana īpašā statusā, ņemot vērā aparātprogrammatūras atjauninājuma sensitīvo drošības raksturu. Šī procesa ietvaros ierīces konfigurācija vai personalizācija, ko persona veikusi, tajā skaitā jebkuri privātuma iestatījumi, var tikt un var arī netikt pārrakstīti un to būs nepieciešams atjaunot. Jebkurā gadījumā LI ierīces aparātprogrammatūras atjaunināšana var būt ļoti sarežģīta parastajam lietotājam.

[6] Drošības pārkāpums tiek definēts kā negatīvas ietekmes radīšana uz konfidencialitāti vai pieejamību.

Aparātprogrammatūras atjaunināšanas problēmas

Pastāv vairākas problēmas, kas jāņem vērā, lai nodrošinātu uzticamu un drošu aparātprogrammatūras atjaunināšanas procesu, tajā skaitā, bet ne tikai:

1. ierīces var nebūt uzreiz pieejamas vai nu fiziski, vai loģistikas dēļ, padarot aparātprogrammatūras atjauninājumu piegādes sarežģītas vai neiespējamas;
2. ierīces var nebūt iespējams atjaunināt tehnisku ierobežojumu dēļ, tāpēc ierīces fiziski jāmaina pret tādām, kas satur atjauninātu aparātprogrammatūru;
3. heterogēns ierīču tīkls (t.i., no dažādiem ražotājiem) saņems atjauninājumus pēc atšķirīga grafika, un ievainojamības tiks fiksētas pēc dažādām skalām (vai netiks fiksētas vispār), kopumā pastāvīgi apdraudot tīkla drošību;
4. īpašumtiesības vai atbildība par ierīču atjaunināšanu, kas piešķirta vairākām organizācijām un personām, nav skaidras vai nedefinētas;
5. personas jāinformē, ka aparātprogrammatūras atjauninājumi ir pieejami un ka tie jāuzstāda savlaicīgi un konsekventi;
6. aparātprogrammatūras atjauninājumi var izmainīt ierīces funkcionalitāti negaidītos un nevēlamos veidos;
7. aparātprogrammatūras atjauninājumi var radīt kļūdas, kas savukārt var ierīci padarīt nelietojamu, ko nav iespējams izlabot vēlāk (piemēram, ierīce var būt "kļūdaina");
8. pat ja jāatjaunina tikai daļa aparātprogrammatūras koda, atjaunināšanas mehānisms var neatbalstīt daļējus vai diferencētus atjauninājumus;
9. aparātprogrammatūras atjaunināšanas process var būt ievainojams un pakļauts manipulācijām (piemēram, publicētā aparātprogrammatūras attēla vietā netīšām var tikt uzstādīts manipulēts kods no neuzticamiem avotiem, kas var radīt drošības pārkāpumus vai ierīces drošības politikas pārkāpumu);
10. sākotnējais ražotājs vairs neatbalsta ierīci, un plānotais aparātprogrammatūras atjauninājums vairs nebūs pieejams;
11. ja ierīci nav iespējams atjaunināt vai pārkāpta tās drošības politika, tā, iespējams, jāizolē no tīkla; un
12. ja aparātprogrammatūras atjaunināšanas process ir sarežģīts vai laikietilpīgs, personas var izvēlēties neuzstādīt atjauninājumu un nesaņemt nelielu privātuma un drošības līmeņa palielinājumu, ko piedāvā atjauninājums, īpaši, ja personas nesaprot, kā atjauninājums padara ierīci drošāku.[7]

[7] Skatīt Aruneš Mathur un Maršini Četi /*Arunesh Mathur & Marshini Chetty*/, *Lietotāja rakstura ietekme uz attieksmi pret automātiskiem mobilo lietotņu atjauninājumiem /Impact of User Characteristics on Attitudes Towards Automatic Mobile Application Updates/*, Trīspadsmitais simpozijs par privātumu un drošību, 175. lpp., 2017. gada 12. līdz 14. jūlijam, https://www.usenix.org/system/files/conference/soups2017/soups2017-mathur.pdf (mobilo lietotņu atjauninājumi). Skatīt Kami Veniea & Jasmīns Rašidi /*Kami Vaniea & Yasmeen Rashidi*/, *Programmatūras atjauninājumu stāsti: programmatūras atjaunināšanas process* /*Tales of Software Updates: The Process of Updating Software*/, 2016., https://vaniea.com/papers/chi2016.pdf (galda datora atjauninājumi) un M. Fagans /*M. Fagan*/, et al., *Pētījums par lietotāju pieredzi un uzskatiem par programmatūras atjauninājumu ziņojumiem /A Study of Users' Experiences and Beliefs About Software Update Messges/*, 51 Žurnāls par datoriem cilvēku uzvedībā /*J. of Computers in Human Behavior*/ 504 (2015), https://dl.acm.org/citation.cfm?id=2805432 (same).

Privātums un datu aizsardzības riski

R1. Ierīces aparātprogrammatūras ievainojamības var sniegt uzbrucējiem tiešu piekļuvi ierīces sensoriem, atļaujot uzbrucējiem aktivizēt sensorus un iegūt sensoru datus (piemēram, kameras attēlus vai audio ierakstus) vai atjaunot šādus datus, ja tie tiek glabāti ierīcē. Skaidri mērķi ir ierīces, kas tiek kontrolētas ar balsi, IP kameras[8] un pat rotaļlietas[9].

R2. Uzbrucēji var mēģināt izmantot LI ierīču ievainojamības, lai iegūtu kontroli pār šīm ierīcēm un lietotu tās kā starpniekserveri turpmākām prettiesiskām darbībām, kas rada privātuma un datu aizsardzības riskus.[10]

R3. Tāpat uzbrucēji var mēģināt piekļūt citiem uzglabātajiem datiem, kas ir atvasināti no sensora datiem, piemēram, norādes par to, kad noteikta persona atradās ierīces tuvumā.

R4. Tāpat uzbrucēji var iegūt akreditācijas datus, kas tiek uzglabāti ierīcē, lai piekļūtu fona sistēmām un piekļūt tur uzglabātajiem sensora datiem, vai arī uzbrucēji var iegūt vai manipulēt ar kriptogrāfiskajām atslēgām, kas tiek izmantotas, lai aizsargātu ierīces komunikāciju, lai atļautu iegūt datus tranzītā.

R5. Ja LI ierīce atrodas privātā mājoklī, sensors un atvasinātie dati var saturēt informāciju par cilvēku, kas atrodas mājsaimniecībā, ikdienu, viņu uzvedību un ieradumiem. Informācija var attiekties uz ilgākiem laika periodiem, taču to var iegūt ar vienu piekļuves darbību.

R6. Mājokļos esošas LI ierīces var uzglabāt arī personu akreditācijas datus (piemēram, tos datus, kas tiek izmantoti e-pastu nosūtīšanai vai informācijas publicēšanai sociālajos tīklos personas vārdā), kas var krist par upuri uzbrukumam. Šie akreditācijas dati sniegtu iespēju veikt arī turpmākas ielaušanās.

Ieteikumi

Izvērtējot aparātprogrammatūras atjauninājumus LI vadības sistēmu kontekstā, būtiski ņemt vērā drošības un datu privātuma aspektus kopumā. Galvenais izaicinājums ir piemērot vienas un tās pašas drošības prakses, kas IT nozarē parasti tiek izmantotas cīņā pret drošības apdraudējumiem (piemēram, droša palaišana, piekļuves kontrole, ierīces autentifikācija, ugunsmūris un ielaušanās aizsardzības sistēmas un atjauninājumi), un piemērot tās arī LI domēnam.

Lai risinātu šajā Darba dokumentā minētās problēmas, tika izstrādāti šādi ieteikumi:

Regulatori, likumdevēji un uzraudzības iestāde

M1. Veicināt aparātprogrammatūras atjauninājumu mehānismu izstrādi un ieviešanu vadības sistēmās;

M2. Veicināt centienus izglītot uzņēmumus un personas par problēmām, kas saistītas ar aparātprogrammatūras atjauninājumiem;

M3. Veicināt projektu ieviešanu, kas pievēršas ierīces drošības ievainojamībām;[11]

---

[8] http://securityaffairs.co/wordpress/50929/malware/linux-mirai-elf.html

[9] Bundesnetzagentur izņem bērnu lelli “Cayla” no tirgushttps://www.bundesnetzagentur.de/SharedDocs/Pressemitteilungen/EN/2017/17022017_cayla.html?nn=404422

[10] https://krebsonsecurity.com/2016/iot-devices-as-proxies-for-cybercrime/

[11] Federālā tirdzniecības komisija (FTK) rīkoja konkursu, kurā sabiedrība tika aicināta izstrādāt tehnisku risinājumu vai rīkus, ko patērētāji varētu izmantot, lai nodrošinātu aizsardzību pret

M4. Izstrādāt prasības LI ierīču drošībai, kas tiek pārdotas personām, kas ietver pienākumu sniegt informāciju par uzstādīto aparātprogrammatūru, par laika periodu, kurā ierīču aparātprogrammatūras atjauninājumi ir pieejami saistībā ar zināmajām ievainojamībām, un par procedūru, kas personām jāievēro, lai garantētu, ka produktam tiek piemēroti jaunākie drošības atjauninājumi; un
M5. Izstrādāt LI aparātprogrammatūras atjaunināšanas procedūras sertifikācijas prasības atbilstoši attiecīgās nozares standartiem. Šiem standartiem jāņem vērā dažādie LI ierīču veidi. Sertifikācijas mērķis ir novērst dažādus riskus un ieviest drošības un privātuma kontroles programmatūras atjauninājumos.

Ierīču ražotāji
M6. Izstrādāt un ieviest drošu aparātprogrammatūras atjaunināšanas mehānismu ierīcēm, kas ietver iespēju viegli un ātri izmantot atjauninājumus, īpaši automātiskus atjauninājumus, kas samazina personām piemēroto slogu;
M7. Ja aparātprogrammatūras atjaunināšanas process var tikt nodrošināts automātiski, jāņem vērā privātumam un drošībai draudzīgi noklusējuma iestatījumi un konfigurācijas opcijas, ko persona iepriekš iestatījusi, vienlaikus iekļaujot noteikumus, kas ļauj personām izvēlēties, kurus atjauninājumus izmantot un no kuriem atteikties, kā arī atjauninājumu laiku;
M8. Izvērtēt, vai atjaunināšanas mehānismam nepieciešami tikai atjauninājumi, ko nodrošina pilnvarotās personas, var tikt uzstādīti (automātiski vai citādi) uz autorizētām ierīcēm un nodrošinātu koda integritāti;
M9. Nodrošināt atbilstošu informāciju personām par drošības apdraudējumiem, kas saistīti ar atjauninājumu uzstādīšanu no neautorizētiem avotiem, kā arī par apdraudējumiem, kas var rasties, neuzstādot autorizētus atjauninājumus, kā arī par priekšrocībām, kas tiek nodrošinātas, uzstādot atjauninājumus vai iespējojot automātiskus atjauninājumus;
M10. Izstrādāt un/vai izmantot atvērtus standartus vienotai funkcionalitātei, piemēram, kriptogrāfiju un tīkla savienojamību;
M11. Piemērot vispārpieņemtus labākās prakses principus drošības un privātuma riska izvērtēšanai kā daļu no ierīces izstrādes dzīves cikla;
M12. Nodrošināt, ka visas trešās personas – piegādātāji nodrošina pastāvīgu atbalstu jebkurai aparātprogrammatūrai, kas varētu tikt ietverta komponentēs, ko tie piegādā ražotājam.
M13. Informēt personas par uzstādīto aparātprogrammatūru, par laika periodu, kurā ierīču aparātprogrammatūras atjauninājumi ir pieejami saistībā ar zināmajām ievainojamībām, un par procedūru, kas personām jāievēro, lai garantētu, ka produktam tiek piemēroti jaunākie drošības atjauninājumi;
M14. Izstrādāt un paziņot par drošības atbalsta periodu visām izstrādātajām ierīcēm. Pirms pirkuma veikšanas izstāstīt personām, kādu drošības atbalstu tās saņems, un atgādināt, kad drošības atbalsts beigsies;

---

drošības ievainojamībām programmatūrās, kas atrastas lietu interneta (LI) ierīcēs viņu mājokļos. https://www.ftc.gov/iot-home-inspector-challenge.

M15. Nodrošināt savlaicīgus atjauninājumus visām ierīcēm to lietošanas laikā, kad tām tiek nodrošināts atbalsts;
M16. Izvērtēt zemu izmaksu alternatīvas pastāvīgam atbalstam, piemēram, pirmkoda izlaišanu, izmantojot atvērtā avota licenci tām ierīcēm, kuru lietošanas laiks ir beidzies;
M17. Piemērot caurskatāmu pieeju atjauninājumiem, nodrošinot pilnu un visaptverošu informāciju par kļūdu labošanu un jaunas funkcijas programmatūras atjauninājumos, un jebkuras izmaiņas atrašanās vietā, kur notiek apstrāde, saistībā ar aparātprogrammatūras atjauninājumu;
M18. Sniegt personām informāciju par aparātprogrammatūras ievainojamībām un sniegt informāciju, kā novērst riskus, kamēr tiek izstrādāti atjauninājumi; un
M19. Pietiekami testēt visu aparātprogrammatūru pirms tās lietošanas un rūpīgi testēt visus atjauninājumus atbilstoši tikpat augstiem standartiem.

Ierīču īpašnieki (organizācijas)

M20. Iegādāties tikai ierīces, kuru ražotāji savlaicīgi nodrošina drošības informāciju un aparātprogrammatūras atjauninājumus, vai novērst jebkurus iespējamos riskus, kas varētu rasties saistībā ar aparātprogrammatūras ievainojamībām jebkādā citā atbilstoši definētā veidā;
M21. Organizācijām jānodrošina aktīvu saraksts, lai būtu iespējams ierīces atrast gan fiziski, gan loģiski;
M22. Organizācijām jāuztur arhitektūras informācija par to sistēmām, drošības pasākumiem, ko tās ieviesušas, un ierīču veiktās datu apstrādes apjoms un raksturs (tajā skaitā apstrādes pamatojums);
M23. Organizācijām jānodrošina, ka tās ir informētas par drošības ievainojamības paziņojumiem, ko publicē ierīces ražotāji, un savlaicīgi jārīkojas atbilstoši šiem brīdinājumiem;
M24. Organizācijām jābūt dokumentētam un pārbaudāmam aparātprogrammatūras atjauninājumu uzstādīšanas procesam visu veidu ierīcēs, tajā skaitā dažādu ražotāju ierīcēs, kas ietver integritātes pārbaudes attiecībā uz jebkuriem atjauninājumiem, kas tiks izlaisti, un jāpārbauda, ka tiek piemēroti ar drošību un privātumu saistīti konfigurācijas iestatījumi vai, ja nepieciešams, iestatīti no jauna pēc atjauninājumu izlaišanas;
M25. Organizācijām pirms uzstādīšanas jāizvērtē, vai nepieciešama turpmāka ražotāja veikta testēšana, izņemot to, ko veic ierīce;
M26. Ja organizācija nolemj, ka aparātprogrammatūras atjauninājuma uzstādīšana ir neatbilstoša, šis lēmums jādokumentē līdz ar piemērotajiem risku novēršanas pasākumiem; un
M27. Organizācijām jābūt definētai politikai, kurā izklāstīts ierīču izslēgšanas, izolēšanas un/vai karantīnas process no pārējā tīkla, ja tiek konstatēta būtiska ievainojamība vai drošības pārkāpums, vai tad, kad ierīces ražotājs pārtrauc sniegt drošības informāciju un atjauninājumus produktam.

Ierīču īpašnieki (personas)

M28. Personām jāsazinās ar ierīces ražotāju, ja tām ir jautājumi par aparātprogrammatūras atjauninājumiem attiecībā uz tiem piederošajām ierīcēm;

M29. Personām jāizvērtē publicētais ierīces lietošanas ilgums un jāapzinās, ka pēc šī datuma, iespējams, nekādi atjauninājumi nebūs pieejami.
M30. Personām jāizvērtē automātisku aparātprogrammatūras atjauninājumu iespējošana (ja šāda opcija ir pieejama) vai citādi jānodrošina, ka ierīču aparātprogrammatūra ir atjaunināta;
M31. Personām jāiegūst aparātprogrammatūras atjauninājumi tikai no uzticamiem avotiem (piemēram, no ierīces ražotāja tīmekļa vietnes) vai, izmantojot nodrošināto droša atjauninājuma mehānismu, un jāpārliecinās par to integritāti, ja tas iespējams; un
M32. Personām jāapzinās, ka atteikšanās no aparātprogrammatūras atjauninājuma, iespējams, baidoties no funkcionalitātes vai stabilitātes zuduma, pakļauj pašu ierīci un plašāku tīklu nevajadzīgām drošības ievainojamībām un tādējādi rada papildu risku sev un pārējiem, kas nonāk kontaktā ar ierīci.