IEC 62443-4-1:2018 Drošs produktu izstrādes dzīves cikls rūpnieciskajā automatizācijā

Drošas izstrādes dzīves cikls, astoņas prakses

47 prasības. Pēc šī standarta ir iespējams sertificēties akreditētā sertifikācijas institūcijā. Redakcija 07/2026.

IEC 62443-4-1 ir sertificējama, taču sertifikācijas objekts ir neparasts: sertificē nosauktas izstrādes organizācijas izstrādes procesu, proti, vienu konkrētu dokumentētu drošā dzīves cikla redakciju. Netiek sertificēts ne produkts, ne persona. Ceļi ir ISASecure SDLA un IECEE CB Scheme. Pēc pašreizējā stāvokļa šāds sertifikāts nerada atbilstības prezumpciju Eiropas Savienības Kibernoturības aktam. Nejaukt ar IEC 62443-4-2, kas izvirza prasības pašam komponentam. Šis saraksts ir darba rīks pašnovērtējumam, nevis pierādījums.

Uzņēmums	Datums	Aizpildīja

5 1. prakse: drošības pārvaldība (SM) 13

SM-1 **Pastāv noteikts produkta izstrādes dzīves cikls, kas drošību ietver katrā posmā, sākot no sākotnējās ieceres līdz produkta izņemšanai no ekspluatācijas, un praksē tiek ievērots tieši šis dzīves cikls.** Dokuments

Pēc kā to var atpazīt: Procesa apraksts vai darba instrukcija, kas uzskaita posmus, katra posma nodevumus un nodošanas punktus, kopā ar pierādījumu no notiekoša projekta, kas apliecina, ka posmi patiešām ir izieti. Mazs uzņēmums iztiek ar vienu lappusi katram posmam un kontrolsarakstu pieteikumu sistēmā; būtiski, ka dokumentētais process un ikdienas prakse sakrīt.

◯ Atvērta ◯ Procesā ◯ Izpildīta ◯ Neattiecas

Pierādījums / pamatojums

SM-2 **Katram drošas izstrādes dzīves cikla uzdevumam ir noteikts atbildīgais, un šis sadalījums ir zināms iesaistītajiem cilvēkiem.** Dokuments

Pēc kā to var atpazīt: Lomu un atbildības matrica, kas katram procesa solim piekārto nosauktu lomu, papildināta ar šo lomu pašreizējo personālsastāvu. Ja cilvēku ir tikai daži, pietiek ar tabulu, kurā ir loma, uzdevums un persona; svarīgākā daļa ir aizvietošanas kārtība atvaļinājuma un slimības laikā.

◯ Atvērta ◯ Procesā ◯ Izpildīta ◯ Neattiecas

Pierādījums / pamatojums

SM-3 **Ir izsekojami noteikts, kuri produkti, varianti, laidieni un komponenti ietilpst drošas izstrādes dzīves ciklā un kuri ne.** Dokuments

Pēc kā to var atpazīt: Tvērumā iekļauto produktu un versiju stāvokļu saraksts ar pamatojumu par iekļaušanu un izslēgšanu, kas tiek uzturēts ar katru jaunu laidienu. Praksē labi darbojas kolonna produktu pārskatā, kurā katrā rindā ir jā vai nē un viens pamatojuma teikums.

◯ Atvērta ◯ Procesā ◯ Izpildīta ◯ Neattiecas

Pierādījums / pamatojums

SM-4 **Cilvēkiem, kas uzņemas drošības uzdevumus, ir tiem nepieciešamā tehniskā kompetence, un šī kompetence tiek mērķtiecīgi veidota un atjaunota.**

Pēc kā to var atpazīt: Kompetences profils katrai drošības lomai, kvalifikācijas ieraksti, apmācību plāns un apmeklējuma ieraksti, papildināti ar trūkumu pārskatu. Mazi uzņēmumi to pierāda ar sertifikātiem, konferenču vai tīmekļa semināru apmeklējumu un īsu ikgadēju pārskatīšanu par to, kurš kuru trūkumu novērš līdz kuram termiņam, nepieciešamības gadījumā piesaistot ārēju zinātību.

◯ Atvērta ◯ Procesā ◯ Izpildīta ◯ Neattiecas

Pierādījums / pamatojums

SM-5 **Drošas izstrādes dzīves cikla tvērums ir norobežots un nosauc iesaistītās atrašanās vietas, organizatoriskās vienības, piegādātāju ieguldījumu un izstrādes vides, kā arī šī tvēruma robežas.** Dokuments

Pēc kā to var atpazīt: Tvēruma apraksts, kas aptver atrašanās vietas, komandas, ārpakalpojumā nodotās daļas un sistēmas, kā arī ārējo saskarņu skice. Ikviens, kas izstrādā vienā atrašanās vietā, to pieraksta dažos teikumos un skaidri nosauc, kas paliek ārpusē, piemēram, ārēji izstrādāti mezgli vai trešās puses mitināšana.

◯ Atvērta ◯ Procesā ◯ Izpildīta ◯ Neattiecas

Pierādījums / pamatojums

SM-6 **Katram lietotājiem piegādātajam elementam, proti, programmatūrai, aparātprogrammatūrai, konfigurācijām un pavadošajiem failiem, ir iespējama integritātes pārbaude, lai saņēmēji varētu atklāt nepamanītas izmaiņas.**

Pēc kā to var atpazīt: Paraksti vai publicētas kontrolsummas katrai piegādes pakotnei, metodes apraksts un viens piemērs no reāla laidiena, kopā ar norādījumiem klientam, kā veikt pārbaudi. Mazām komandām pietiek ar parakstītu kontrolsummu failu blakus lejupielādei un rindkopu laidiena piezīmēs.

○ Atvērta ○ Procesā ○ Izpildīta ○ Neattiecas

Pierādījums / pamatojums

SM-7 **Izstrādei, būvēšanai un testēšanai izmantotās vides ir aizsargātas pret nesankcionētu piekļuvi un pret pirmkoda, būvēšanas rīku un artefaktu neatļautu mainīšanu.**

Pēc kā to var atpazīt: Piekļuves pārvaldības koncepcija repozitorijam, būvēšanas serverim un testēšanas sistēmām, piekļuves saraksti ar pēdējās pārskatīšanas datumu, ieraksti par drošībai nozīmīgām izmaiņām un pierādījums, ka piekļuve ražošanas videi un izstrādes videi ir nodalīta. Bez sava informācijas tehnoloģiju departamenta pietiek ar divfaktoru pieteikšanos, aizsargātu galveno zaru ar obligātu pārskatīšanu un reizi pusgadā veiktu pārskatīšanu par to, kam piekļuve vēl ir saglabāta.

○ Atvērta ○ Procesā ○ Izpildīta ○ Neattiecas

Pierādījums / pamatojums

SM-8 **Privātās atslēgas, ar kurām paraksta piegādes, ir aizsargātas pret izpaušanu un ļaunprātīgu izmantošanu, un to lietošana ir ierobežota ar pilnvarotiem cilvēkiem un sistēmām.**

Pēc kā to var atpazīt: Apraksts par atslēgu glabāšanu, piekļuvi, atjaunošanu un atsaukšanu, pierādījums par aizsargātu glabāšanu, piemēram, aparatūras marķierī vai atslēgu pārvaldības pakalpojumā, kā arī ieraksti par parakstīšanas darbībām. Mazs uzņēmums parakstīšanas atslēgu tur aparatūras marķierī, dokumentē divus cilvēkus ar piekļuvi un tur gatavu procedūru nozaudēšanas gadījumam.

○ Atvērta ○ Procesā ○ Izpildīta ○ Neattiecas

Pierādījums / pamatojums

SM-9 **Iepirktiem vai pārņemtiem komponentiem, tostarp atvērtā koda programmatūrai, ir noteiktas piegādātājam izvirzītās drošības prasības, un tās tiek piemērotas izvēles laikā.** Dokuments

Pēc kā to var atpazīt: Drošības prasības piegādātāju specifikācijās vai līgumos, trešās puses komponentu izvēles kritēriji, visu trešās puses komponentu uzskaite ar versiju un avotu, kā arī novērtējums, vai piegādātājs šīs prasības izpilda. Bez iepirkumu daļas pietiek ar uzturētu komponentu sarakstu, kurā kolonna reģistrē, vai ir pārbaudīti piegādātāja drošības atjauninājumi un ziņošanas kanāli.

○ Atvērta ○ Procesā ○ Izpildīta ○ Neattiecas

Pierādījums / pamatojums

SM-10 **Komponentiem, ko pēc pasūtījuma izstrādā trešā puse, ir spēkā tās pašas drošības prasības, kas iekšējai izstrādei, un to ievērošana tiek pārbaudīta.**

Pēc kā to var atpazīt: Pasūtījums vai līguma dokumenti, kas nosaka prasītos drošības pienākumus, pakalpojuma sniedzēja pierādījums par izmantotajām praksēm, pieņemšanas ieraksti un paša uzņēmuma pārbaužu rezultāti par piegādāto darbu. Bez audita budžeta pietiek ar līgumisku apliecinājumu, pakalpojuma sniedzēja testu rezultātu iesniegšanu un vienu paša veiktu izlases pārbaudi pirms pieņemšanas.

○ Atvērta ○ Procesā ○ Izpildīta ○ Neattiecas

Pierādījums / pamatojums

SM-11 **Drošībai nozīmīgi konstatējumi no visiem avotiem, proti, no testiem, pārskatīšanām, lietotāju ziņojumiem un trešo pušu paziņojumiem, tiek fiksēti, novērtēti pēc to ietekmes, tiem tiek noteikta atbildīgā persona un termiņš, un tie tiek izsekoti līdz slēgšanai.** Dokuments

Pēc kā to var atpazīt: Defektu vai pieteikumu sistēma ar atsevišķu apzīmējumu drošības tēmām, un katram ierakstam ietekmes novērtējums, atbildīgā persona, termiņš un slēgšanas piezīme, kā arī pārskats par atvērtajiem punktiem. Maza komanda izmanto iezīmi esošajā pieteikumu sistēmā un pastāvīgu darba kārtības punktu iknedēļas sanāksmē.

○ Atvērta ○ Procesā ○ Izpildīta ○ Neattiecas

Pierādījums / pamatojums

SM-12 **Pirms produkta laidiena tiek pārbaudīts un pierādīts, ka drošas izstrādes dzīves cikla paredzētie soļi patiešām ir veikti un ka ir izveidoti attiecīgie ieraksti.** Dokuments

Pēc kā to var atpazīt: Laidiena pārskatīšana katram laidienam, salīdzinot ar procesa soļiem, atsauces uz attiecīgajiem ierakstiem un dokumentēts lēmums par laidienu ar datumu un parakstu. Praksē labi darbojas laidiena kontrolsaraksts, kas nepieļauj piegādi bez pilnībā atzīmētiem punktiem; atvērtie punkti tiek pamatoti un tiem tiek noteikts datums.

◯ Atvērta ◯ Procesā ◯ Izpildīta ◯ Neattiecas

Pierādījums / pamatojums

SM-13 **Pats drošas izstrādes dzīves cikls tiek regulāri pārvērtēts un uzlabots, izmantojot atziņas no notikumiem, testu rezultātiem, klientu atsauksmēm un apdraudējumu ainas.**

Pēc kā to var atpazīt: Ieraksti par procesa pārskatīšanu, piemēram, vadības pārskatīšana vai retrospektīva, ar ierosinātajām procesa izmaiņām, to ieviešanas statusu un atsauci uz pamatcēloni. Ikviens, kas izmanto standarta brieduma līmeņus, katrai praksei pieraksta pašreizējo un mērķa stāvokli; brieduma līmenis 4 prasa tieši šo pierādījumu par nepārtrauktu uzlabošanu. Mazam uzņēmumam pietiek ar vienu sanāksmi gadā ar protokolu un trim konkrētiem uzlabojumiem.

◯ Atvērta ◯ Procesā ◯ Izpildīta ◯ Neattiecas

Pierādījums / pamatojums

6 2. prakse: drošības prasību specificēšana (SR) 5

SR-1 **Paredzētais produkta konteksts ir aprakstīts: sagaidāmā ekspluatācijas vide, drošības pasākumi, ko pieņem par šīs vides nodrošinātiem, paredzētās lietotāju grupas un lomas, pieņemtās uzticamības robežas un lietojumi, kuriem produkts skaidri nav paredzēts.** Dokuments

Pēc kā to var atpazīt: Produkta drošības konteksta apraksts vai nu kā atsevišķs dokuments, vai kā pastāvīga produkta specifikācijas sadaļa, kas aptver tīkla vidi, pieņemtos ārējos aizsardzības pasākumus, piemēram, ugunsmūri vai fizisku piekļuves pārvaldību, lomu sarakstu un skaidru sarakstu ar lietojumiem ārpus tvēruma. Mazs uzņēmums to ietver divās lappusēs, pievieno vienkāršu iekārtas vides skici, un produkta īpašnieks to datē un apstiprina.

◯ Atvērta ◯ Procesā ◯ Izpildīta ◯ Neattiecas

Pierādījums / pamatojums

SR-2 **Produktam pastāv apdraudējumu modelis, kas attēlo datu plūsmas, saskarnes, uzticamības robežas un uzbrukuma ceļus, nosauc no tiem izrietošos apdraudējumus un to iespējamo ietekmi un piekārto pretpasākumus. Tas tiek pārskatīts un atjaunināts būtisku izmaiņu gadījumā un vismaz reizi katrā produkta laidienā, un atvērtie punkti tiek izsekoti līdz to slēgšanai.** Dokuments

Pēc kā to var atpazīt: Apdraudējumu modelis ar datu plūsmas diagrammu, apdraudējumu sarakstu katrai saskarnei, piekārtotiem pretpasākumiem un atvērto punktu statusu, kā arī izmaiņu vēsture ar datumu un autoru. Mazs uzņēmums var strādāt ar vienu tabulu katrai saskarnei, kurā kolonnas atbild uz to, kas tur var noiet greizi, cik smagi tas būtu, ko uzņēmums dara, lai to novērstu, un kurš to pārskata.

◯ Atvērta ◯ Procesā ◯ Izpildīta ◯ Neattiecas

Pierādījums / pamatojums

SR-3 **Produkta drošības prasības ir noteiktas un dokumentētas. Tās aptver apdraudējumu modeļa rezultātus, aprakstīto produkta drošības kontekstu, piemērojamos tiesiskos un līgumiskos pienākumus un mērķa drošības līmeni, un tās ietver drošības spējas, ko nodrošina pats produkts.** Dokuments

Pēc kā to var atpazīt: Prasību saraksts vai prasību pārvaldības rīks ar unikālu identifikatoru katrai prasībai, katra ieraksta avotu, piemēram, apdraudējumu, klienta līgumu vai tiesisku pienākumu, un mērķa drošības līmeni. Mazs uzņēmums to uztur kā vienu tabulu ar pastāvīgu identifikatora kolonnu, pie kuras vēlāk piesaistās verifikācija un testēšana.

◯ Atvērta ◯ Procesā ◯ Izpildīta ◯ Neattiecas

Pierādījums / pamatojums

SR-4 **Katra atsevišķa drošības prasība ir formulēta tā, ka tā ir nepārprotama, bez pretrunām, testējama un izsekojama līdz konkrētai produkta funkcijai vai saskarnei, un tā satur informāciju, kas nepieciešama tās vēlākai pārbaudei bez papildu skaidrojumiem.**

Pēc kā to var atpazīt: Izlase no prasību saraksta, kas katrai prasībai rāda izmērāmu pieņemšanas kritēriju un skarto funkciju vai saskarni, kopā ar prasību un testa gadījumu piekārtojumu. Mazs uzņēmums to pārbauda ar pastāvīgu formulējuma veidni un kontroljautājumu, vai no prasības var uzrakstīt testa gadījumu bez papildu jautājumiem.

◯ Atvērta ◯ Procesā ◯ Izpildīta ◯ Neattiecas

Pierādījums / pamatojums

SR-5 **Drošības prasības tiek pārskatītas, pirms tās izmanto projektēšanā un īstenošanā, iesaistot skartās puses, piemēram, izstrādi, testēšanu, produkta īpašnieku un, kur lietderīgi, pārdošanu vai klientu. Pārskatīšana aptver pilnīgumu attiecībā pret apdraudējumu modeli un produkta drošības kontekstu, pareizību un testējamību. Konstatējumi tiek reģistrēti un izsekoti līdz slēgšanai.**

Pēc kā to var atpazīt: Pārskatīšanas ieraksts ar datumu, dalībniekiem un to lomām, pārskatīto prasību versiju, konstatējumu sarakstu ar atbildīgo personu un slēgšanas statusu, kā arī apstiprinājuma piezīmi. Mazs uzņēmums to risina kā divu cilvēku pārskatīšanu starp izstrādi un testēšanu, ar īsu ierakstu un apstiprinājuma rindu prasību sarakstā.

○ Atvērta ○ Procesā ○ Izpildīta ○ Neattiecas

Pierādījums / pamatojums

7 3. prakse: droša projektēšana (SD) 4

SD-1 **Katram produktam ir projekta apraksts, kas atspoguļo arhitektūras drošībai nozīmīgos aspektus: kādi komponenti pastāv, kā tie savstarpēji sazinās, kur iet uzticamības robežas, kādas ārējās saskarnes ir pieejamas un ar kādiem mehānismiem projektā ir īstenotas iepriekš noteiktās drošības prasības.** Dokuments

Pēc kā to var atpazīt: Arhitektūras dokuments vai projekta specifikācija ar diagrammu, kas rāda komponentus, datu plūsmas un uzticamības robežas, kā arī piekārtojuma tabula no katras drošības prasības uz projekta elementu, kas to īsteno. Mazs piegādātājs iztiek ar vienu uzturētu diagrammu un divām vai trim skaidrojuma lappusēm; būtiski, ka tā ir versiju kontrolē repozitorijā un tiek atjaunināta ikreiz, kad mainās arhitektūra.

○ Atvērta ○ Procesā ○ Izpildīta ○ Neattiecas

Pierādījums / pamatojums

SD-2 **Projekts tiek sistemātiski analizēts attiecībā uz apdraudējumiem. Analīze nosauc uzbrucēja mērķus, skartās uzticamības robežas un saskarnes, no tā izrietošos apdraudējumus kopā ar to novērtējumu un projektā veiktos pretpasākumus. Tā tiek atkārtota ikreiz, kad būtiski mainās arhitektūra vai vide, un apzinātie apdraudējumi tiek izsekoti, līdz par katru no tiem ir pieņemts lēmums.** Dokuments

Pēc kā to var atpazīt: Apdraudējumu modelis katram produktam vai katram lielajam laidienam, piemēram, tabula ar kolonnām apdraudējums, skartā saskarne, novērtējums, pretpasākums un statuss, kopā ar modelēšanas sanāksmes protokolu, kurā uzskaitīti dalībnieki un datums. Maza komanda modelē pragmatiski divu līdz trīs stundu darbnīcā pēc arhitektūras diagrammas un atvērtos punktus pieraksta kā pieteikumus, tādēļ pierādījums par izsekošanu rodas bez papildu pūlēm.

○ Atvērta ○ Procesā ○ Izpildīta ○ Neattiecas

Pierādījums / pamatojums

SD-3 **Projekts pierādāmi ievēro atzītus drošas projektēšanas principus, tostarp mazāko privilēģiju principu, minimālu uzbrukuma virsmu, daudzslāņu aizsardzību, drošas noklusējuma vērtības, drošu uzvedību atteices gadījumā un pēc iespējas vienkāršus un pārbaudāmus drošības mehānismus. Šo principu piemērošana ir redzama projektā un pamatota.**

Pēc kā to var atpazīt: Sadaļa projekta aprakstā vai iekšēja projektēšanas vadlīnija, kas nosauc principus, kā arī konkrēts pierādījums par katru principu produktā, piemēram, pakalpojumu privilēģiju matrica, atvērto portu saraksts ar pamatojumu, piegādes noklusējuma vērtības vai dokumentētā kļūdu apstrādes uzvedība. Mazs piegādātājs izmanto īsu šo principu kontrolsarakstu kā pastāvīgu punktu projekta pārskatīšanā un aizpildīto lapu glabā kopā ar projektu.

○ Atvērta ○ Procesā ○ Izpildīta ○ Neattiecas

Pierādījums / pamatojums

SD-4 **Projektu pirms īstenošanas sākuma pārskata kvalificēti kolēģi. Pārskatīšana aptver pilnīgumu attiecībā pret drošības prasībām, drošības mehānismu pareizību un rezultativitāti un apdraudējumu analīzes rezultātus. Piedalās cilvēki ar pietiekamu drošības kompetenci, konstatējumi tiek reģistrēti un izsekoti līdz slēgšanai.** Dokuments

Pēc kā to var atpazīt: Pārskatīšanas ieraksts ar datumu, pārskatāmo objektu un tā versiju, dalībniekiem un to lomām, konstatējumu sarakstu ar statusu un apstiprinājuma lēmumu. Maza komanda pārskatīšanu pievieno projekta dokumentu izmaiņu pieprasījumam un konstatējumus atstāj kā komentārus ar slēgšanas piezīmi, kas pierāda izsekošanu bez papildu rīkiem. Ja iekšēji trūkst drošības kompetences, pragmatisks ceļš ir ārējs pārskatītājs, ko kritiskajiem projektiem piesaista uz stundu apmaksas pamata.

○ Atvērta ○ Procesā ○ Izpildīta ○ Neattiecas

Pierādījums / pamatojums

8 4. prakse: droša īstenošana (SI) 2

SI-1 **Pastāv noteikts process faktiskās īstenošanas pārbaudei pret drošo projektu: pārskatīšana apstiprina, ka projektā paredzētie aizsardzības pasākumi kodā patiešām pastāv un ir rezultatīvi, ka daudzslāņu aizsardzība ir saglabāta un ka īstenošanas laikā nav radītas jaunas ievainojamības. Pārskatīšanu veic atbilstoši kvalificēts personāls, un konstatētās novirzes tiek reģistrētas un izsekotas līdz slēgšanai.**

Pēc kā to var atpazīt: Rakstiska īstenošanas pārskatīšanas procedūra kopā ar pārskatīšanas ierakstiem par katru komponentu vai laidienu: pārskatītais modulis, atsauce uz projekta dokumentu, datums, pārskatītājs, konstatējumi un to novēršanas statuss. Piemērots pierādījums ir izmaiņu pieprasījumu pārskatīšana ar obligātu drošības kontrolsarakstu, statiskās koda analīzes rezultāti ar dokumentētu novērtējumu par katru atradumu un pārskatīšanas sanāksmju protokoli. Maza komanda to sedz ar četru acu principu, repozitorijā glabātu pārskatīšanas veidni, kurā katrs projekta pasākums tiek atzīmēts atsevišķi, un vienu pieteikumu katram atvērtajam konstatējumam. Būtiski, ka koda autors nekad nav tā paša koda pārskatītājs.

◯ Atvērta ◯ Procesā ◯ Izpildīta ◯ Neattiecas

Pierādījums / pamatojums

SI-2 **Visam drošībai nozīmīgajam izstrādes darbam ir spēkā saistoši drošas kodēšanas noteikumi, kas aptver vismaz izvairīšanos no zināmām nedrošām konstrukcijām un funkcijām, ievaddatu un kļūdu apstrādi, atmiņas un resursu pārvaldību un pārbaudīta drošības koda izmantošanu pašu rakstītu risinājumu vietā. Noteikumi ir spēkā katrai lietotajai programmēšanas valodai, ir zināmi visiem izstrādātājiem un tiek atjaunināti pēc vajadzības, piemēram, kad parādās jauni uzbrukumu paņēmieni vai jauni rīki.**

Dokuments

Pēc kā to var atpazīt: Apstiprināts drošas kodēšanas standarts ar versijas stāvokli, tvērumu katrai valodai un apstiprināšanas datumu, papildināts ar pierādījumu, ka tas darbojas ikdienā: koda pārbaudes un analīzes rīku konfigurācija repozitorijā, būvēšanas noteikums, kas parāda pārkāpumus, un instruktāžas apmeklējuma saraksts. Mazi uzņēmumi standartu neraksta no nulles; tie par saistošu atzīst nostiprinājušos publisku noteikumu kopumu, pievieno īsu savu papildu noteikumu sarakstu un pārbaudi nostiprina konveijerā, tā ka ievērošana tiek pierādīta automātiski.

◯ Atvērta ◯ Procesā ◯ Izpildīta ◯ Neattiecas

Pierādījums / pamatojums

9 5. prakse: drošības verifikācijas un validācijas testēšana (SVV) 5

SVV-1 **Katrai drošībai nozīmīgai produkta prasībai ir piekārtots vismaz viens testa gadījums, kas apliecina, ka aizsardzības funkcija normālā darbībā strādā, kā paredzēts, ka tā uzvedas atbilstoši specifikācijai, saņemot nederīgus ievaddatus vai tiekot ļaunprātīgi izmantota, un ka produkta piegādes noklusējuma iestatījumi atbilst drošam stāvoklim. Izpilde un rezultāts tiek reģistrēti katrai testētajai programmatūras versijai.**

Dokuments

Pēc kā to var atpazīt: Izsekojamības matrica, kas saista prasību ar testa gadījumu un rezultātu, kā arī testu ieraksti, kuros redzams datums, testētā versija vai būvējums un testa veicēja vārds. Mazs piegādātājs savam prasību sarakstam vienkārši pievieno testa gadījuma identifikatora kolonnu un automatizētā testa izpildes žurnālu no būvēšanas konveijera arhivē kā failu, kas pievienots attiecīgajai versijai.

◯ Atvērta ◯ Procesā ◯ Izpildīta ◯ Neattiecas

Pierādījums / pamatojums

SVV-2 **No apdraudējumu modeļa atvasinātie pretpasākumi tiek mērķtiecīgi testēti, lai apstiprinātu, ka tie patiešām noslēdz pieņemto uzbrukuma ceļu. Testēšana notiek pret apzinātajiem apdraudējumiem, nevis tikai pret pareizu lietošanu, un atvērtie punkti nonāk defektu apstrādes procesā.**

Pēc kā to var atpazīt: Testa gadījumi, kas tieši atsaucas uz apdraudējumu modeļa ierakstiem, piemēram, viens ļaunprātīgas izmantošanas gadījums katram apdraudējuma identifikatoram ar sagaidāmo aizsardzības uzvedību, kopā ar šo izpilžu ierakstiem. Bez sarežģītiem rīkiem pietiek apdraudējumu modelim pievienot kolonnu ar atsauci uz testa gadījumu un pēdējās veiksmīgās pārbaudes datumu.

◯ Atvērta ◯ Procesā ◯ Izpildīta ◯ Neattiecas

Pierādījums / pamatojums

SVV-3 **Produkts pirms laidiena tiek sistemātiski pārbaudīts attiecībā uz ievainojamībām. Tvērums aptver vismaz: no ārpuses sasniedzamo saskarņu un pakalpojumu pārbaudi, testēšanu ar bojātiem un nejauši mainītiem ievaddatiem, izmantoto trešās puses komponentu salīdzināšanu ar zināmām ziņotām ievainojamībām un paša piegādātāja koda pārbaudi attiecībā uz zināmām vājo vietu klasēm. Konstatējumi tiek reģistrēti kopā ar to novērtējumu.** Dokuments

Pēc kā to var atpazīt: Izmantoto rīku atskaites, kurās norādīts rīka nosaukums, versija un ievainojamību datubāzes datu stāvoklis, ieraksti par testēšanu ar nejauši mainītiem ievaddatiem, trešās puses komponentu saraksts ar pēdējās salīdzināšanas datumu un konstatējumu saraksts ar novērtējumu un lēmumu. Mazs piegādātājs apvieno bezmaksas standarta rīkus, atkarību skenēšanu un portu un pakalpojumu skenēšanu pret uzstādīto produktu un izvades katram laidienam glabā vienā mapē.

◯ Atvērta ◯ Procesā ◯ Izpildīta ◯ Neattiecas

Pierādījums / pamatojums

SVV-4 **Laidiena kandidāts tiek pakļauts uzbrukuma mēģinājumam reālistiskos apstākļos, kas aktīvi cenšas apiet aizsardzības mehānismus, nevis tos tikai aptaujā. Testa tvērums, robežnosacījumi un ierobežojumi tiek saskaņoti iepriekš, un atrastās vājās vietas tiek apstrādātas un izsekotas kā defekti.**

Pēc kā to var atpazīt: Uzdevums vai testa pasūtījums, kurā norādīts tvērums un testa vide, atskaite par pieeju, izmantotajām vājajām vietām un to novērtējumu, kā arī ieraksti defektu vai pieteikumu sistēmā ar pierādījumu par novēršanu vai par pamatotu riska pieņemšanu. Mazi piegādātāji šo testu parasti pērk ārpakalpojumā ar ierobežotu laika budžetu vai uztic to personai, kas produktu nav izstrādājusi.

◯ Atvērta ◯ Procesā ◯ Izpildīta ◯ Neattiecas

Pierādījums / pamatojums

SVV-5 **Testēšanas personāla neatkarība ir noteikta un atbilst paredzētajam brieduma līmenim. Komponenta izstrādātājs to neapstiprina laidienam, balstoties vienīgi uz savu testēšanu, un, brieduma līmenim pieaugot, par testēšanu atbild organizatoriski nodalīta vienība vai ārēja puse. Faktiskais sadalījums katram testam ir izsekojams.**

Pēc kā to var atpazīt: Lomu apraksts izstrādes procesā, kas rāda izveides un testēšanas nodalīšanu, kā arī katrai testa izpildei vai testa atskaitei reģistrēts testa veicēja vārds un loma. Divu cilvēku uzņēmums to risina ar savstarpēju pārskatīšanu un dokumentētu četru acu piezīmi un padziļinātai drošības testēšanai piesaista ārēju personu.

◯ Atvērta ◯ Procesā ◯ Izpildīta ◯ Neattiecas

Pierādījums / pamatojums

10 6. prakse: drošības defektu pārvaldība (DM) 6

DM-1 **Pastāv noteikts kanāls, pa kuru no visām pusēm tiek saņemti un reģistrēti ziņojumi par produkta drošības vājajām vietām: no pašas izstrādes komandas, no testēšanas un pārskatīšanām, no klientiem un integratoriem, no ārējiem ziņotājiem un no drošības paziņojumiem par izmantotajiem trešās puses un atvērtā koda komponentiem. Ziņošanas kanāls ir atrodams ārējām pusēm, un katrs ziņojums tiek fiksēts ar saņemšanas datumu un avotu.** Dokuments

Pēc kā to var atpazīt: Ziņošanas kanāla apraksts, publiski sasniedzamais kontaktpunkts (drošības lapa, security.txt fails vai pastkaste, piemēram, security@), un saņemšanas reģistrs, kurā katram ziņojumam ir datums, avots un īss apraksts. Mazs uzņēmums var strādāt ar kopīgu pastkasti un vienu izklājlapu vai pieteikuma iezīmi, ja vien tur nonāk katrs ziņojums, tostarp tie, kas izteikti iekšējā izstrādātāju tērzēšanā.

◯ Atvērta ◯ Procesā ◯ Izpildīta ◯ Neattiecas

Pierādījums / pamatojums

DM-2 **Katrs saņemtais ziņojums tiek sākotnēji izvērtēts un pārbaudīts, lai noteiktu, vai tas ir drošībai nozīmīgs un kurus produktus, versijas un komponentus tas skar. Arī ziņojumi, kas izrādās drošībai nenozīmīgi vai nepiemērojami, tiek slēgti ar norādītu pamatojumu, nevis klusējot atmesti.**

Pēc kā to var atpazīt: Sākotnējā izvērtējuma piezīme katram ziņojumam ar rezultātu (drošībai nozīmīgs jā vai nē), skartajām versijām un noraidīšanas pamatojumu, kur tas ir vajadzīgs, redzama pieteikumā vai saņemšanas sarakstā. Komandas ar nelielu ziņojumu apjomu izvērtējumu var veikt īsā regulārā sanāksmē un rezultātu pierakstīt divos teikumos katram ierakstam.

◯ Atvērta ◯ Procesā ◯ Izpildīta ◯ Neattiecas

Pierādījums / pamatojums

DM-3 **Apstiprinātie drošības defekti tiek novērtēti pēc vienotas metodes: pamatcēlonis, skartās versijas un konfigurācijas, iespējamā ietekme uz darbību un drošību, izmantojamība un smaguma pakāpe pēc noteiktas skalas. Novērtējuma rezultāts tiek reģistrēts un ir izsekojams.** Dokuments

Pēc kā to var atpazīt: Novērtējuma ieraksts vai pieteikuma lauku kopa katram defektam, kas aptver pamatcēloni, smaguma pakāpi un piemēroto skalu (piemēram, vispārpieņemtu smaguma novērtēšanas sistēmu ar dokumentētu vektoru), kopā ar skarto versiju sarakstu. Mazas komandas var paļauties uz pastāvīgu lauku veidni pieteikumu sistēmā un pusi lappuses, kas apraksta skalu un sliekšņus, pēc kuriem seko tūlītēja rīcība.

◯ Atvērta ◯ Procesā ◯ Izpildīta ◯ Neattiecas

Pierādījums / pamatojums

DM-4 **Par katru novērtēto drošības defektu tiek pieņemts lēmums par tā apstrādi: novēršana, kompensējošs pasākums vai pamatota riska pieņemšana. Lēmums izriet no smaguma pakāpes, tam ir noteikta atbildīgā persona un termiņš, un defekts tiek izsekots līdz slēgšanai.** Dokuments

Pēc kā to var atpazīt: Darbību saraksts vai pieteikuma statuss ar atbildīgo personu, mērķa datumu, pasākuma veidu un slēgšanas piezīmi, saistīts ar koda bāzi vai laidienu, kurā labojums stājas spēkā. Pieņemtajiem atlikušajiem riskiem ir nepieciešams īss rakstisks pamatojums, ko apstiprina produkta īpašnieks. Mazs uzņēmums to var uzturēt pieteikumu tāfelē ar termiņiem, bez papildu rīkiem.

◯ Atvērta ◯ Procesā ◯ Izpildīta ◯ Neattiecas

Pierādījums / pamatojums

DM-5 **Skartie lietotāji, integratori un citas ieinteresētās puses tiek informēti par drošības defektiem, tiklīdz to prasa novērtējums, norādot skartās versijas, ietekmi un pieejamo labojumu vai kompensējošo pasākumu. Šādas izpaušanas termiņi un saņēmēju loks ir noteikti iepriekš, tāpat kā rīcība ar trešo pušu ziņojumiem, kuriem ir savs izpaušanas termiņš.**

Pēc kā to var atpazīt: Publicēti drošības ziņojumi vai paziņojumi ar datumu un atsauci uz versiju, izplatīšanas saraksts vai abonentu kanāls un rakstisks noteikums par termiņiem un koordinētu izpaušanu. Piegādātāji ar nedaudziem klientiem var izmantot vienu izsūtījumu uz uzturētu klientu sarakstu un datētu paziņojumu lapu, kuras izmaiņām tiek piešķirtas versijas.

◯ Atvērta ◯ Procesā ◯ Izpildīta ◯ Neattiecas

Pierādījums / pamatojums

DM-6 **Drošības defektu apstrāde tiek pārskatīta noteiktos intervālos. Pārskatīšana aplūko atvērtos un nokavētos gadījumus, laiku no ziņojuma līdz novēršanai, atkārtotus pamatcēloņus un veikto pasākumu rezultativitāti. No pārskatīšanas izrietošie procesa uzlabojumi tiek ieviesti, un to ieviešana tiek izsekota.** Dokuments

Pēc kā to var atpazīt: Regulārās pārskatīšanas protokols ar datumu, dalībniekiem, skaitļiem par atvērtajiem un nokavētajiem gadījumiem un saskaņoto uzlabojumu sarakstu ar atbildīgo personu un termiņu. Mazs uzņēmums šo punktu var pievienot esošai ceturkšņa sanāksmei un skaitļus un lēmumus turēt vienā lappusē.

◯ Atvērta ◯ Procesā ◯ Izpildīta ◯ Neattiecas

Pierādījums / pamatojums

11 7. prakse: drošības atjauninājumu pārvaldība (SUM) 5

SUM-1 **Katrs produkta drošības atjauninājums pirms izlaišanas klientiem tiek pārbaudīts pret atbalstītajām produkta versijām un ekspluatācijas vidēm, un pastāv ieraksts, kas apliecina, ka atjauninājums novērš ievainojamību, netraucējot paredzēto produkta darbību.** Dokuments

Pēc kā to var atpazīt: Testa ieraksts katram ielāpam, kas aptver testēto produkta versiju, platformu, testa gadījumus (rezultativitāte pret ievainojamību un pamatfunkciju regresija) un laidiena apstiprinājumu. Mazs piegādātājs var strādāt ar īsu ielāpa apstiprinājuma ierakstu pieteikumā: pieteikuma identifikators, kas pārbaudīja, kad pārbaudīja, rezultāts, ar pievienotu automatizētā testa izpildes žurnālu.

◯ Atvērta ◯ Procesā ◯ Izpildīta ◯ Neattiecas

Pierādījums / pamatojums

SUM-2 **Visiem produkta komponentiem, kas nav izstrādāti pašu spēkiem (trešās puses bibliotēkas, operētājsistēma, izpildvides), ir noteikts un pierādīts, kā to drošības atjauninājumi tiek novērtēti un vai nu pārņemti produktā, vai noraidīti ar dokumentētu pamatojumu.** Dokuments

Pēc kā to var atpazīt: Trešās puses komponentu uzskaite ar versiju un avotu, kā arī viens novērtējuma ieraksts katrai ziņotajai trešās puses ievainojamībai ar lēmumu (pārņemt, neskar, segts ar kompensējošu pasākumu) un pamatojumu. Mazas komandas būvējumā izpilda automatizētu atkarību skenēšanu un lēmumus glabā kā komentārus pie skenēšanas rezultāta vai vienkāršā izņēmumu sarakstā.

◯ Atvērta ◯ Procesā ◯ Izpildīta ◯ Neattiecas

Pierādījums / pamatojums

SUM-3 **Par katru piegādāto drošības atjauninājumu lietotāji saņem saprotamu pavadinformāciju: kuras produkta versijas ir skartas, kura ievainojamība ir novērsta, cik tā ir smaga, vai pastāv vērā ņemamas blakusparādības vai kompensējoši pasākumi un kā atjauninājums tiek uzstādīts.** Dokuments

Pēc kā to var atpazīt: Publicēti drošības paziņojumi vai laidiena piezīmes ar ievainojamības identifikatoru, skartajām versijām, smaguma novērtējumu, uzstādīšanas soļiem un norādēm par atgriešanos iepriekšējā stāvoklī. Mazi piegādātāji uztur vienu publisku lapu ar hronoloģisku drošības paziņojumu sarakstu un uz to norāda no paša produkta.

◯ Atvērta ◯ Procesā ◯ Izpildīta ◯ Neattiecas

Pierādījums / pamatojums

SUM-4 **Pastāv noteikts un pret neatļautu mainīšanu aizsargāts ceļš, pa kuru lietotāji saņem drošības atjauninājumus, un atjauninājuma autentiskumu un integritāti lietotāja pusē var pārbaudīt pirms uzstādīšanas.**

Pēc kā to var atpazīt: Piegādes kanāla apraksts (lejupielādes sadaļa, atjauninājumu serveris, fiziski datu nesēji) kopā ar tā aizsardzības pasākumiem, kā arī ciparparaksts vai kontrolsumma katrai pakotnei un norādījumi lietotājam, kā to pārbaudīt. Mazi piegādātāji to panāk, parakstot būvēšanas serverī, publicējot kontrolsummu blakus lejupielādei un nosaucot vienu skaidru vietu, kur glabājas publiskā atslēga.

◯ Atvērta ◯ Procesā ◯ Izpildīta ◯ Neattiecas

Pierādījums / pamatojums

SUM-5 **Pastāv noteikti laika mērķi drošības atjauninājumu pieejamībai, sagrupēti pēc ievainojamības smaguma pakāpes; faktiski sasniegtie termiņi tiek izsekoti, un katrs nokavēts mērķis tiek pamatots un papildināts ar pagaidu pasākumu lietotājiem.** Dokuments

Pēc kā to var atpazīt: Iekšēja specifikācija ar laika logu katrai smaguma kategorijai (piemēram, kritiska <= 30 dienas, augsta <= 90 dienas) un izvērtējums katrai ievainojamībai: ziņojuma datums, ielāpa laidiena datums, pagājušās dienas, novirzes iemesls. Mazi piegādātāji to uztur kā divus datuma laukus ievainojamības pieteikumā un sarakstu pārskata reizi ceturksnī, nevis ievieš atsevišķu rādītāju sistēmu.

◯ Atvērta ◯ Procesā ◯ Izpildīta ◯ Neattiecas

Pierādījums / pamatojums

12 8. prakse: drošības vadlīnijas produkta ieviešanai un ekspluatācijai (SG) 7

SG-1 **Katram produktam ir pievienots tā daudzslāņu aizsardzības stratēģijas apraksts: tas nosauc pašā produktā iebūvētos aizsardzības slāņus, piekārto tos apdraudējumiem, pret kuriem tie darbojas, un rāda, kāda aizsardzības ietekme rodas tikai no vairāku slāņu mijiedarbības.** Dokuments

Pēc kā to var atpazīt: Sadaļa piegādātajā produkta dokumentācijā vai atsevišķa drošības koncepcija, kas katram aizsardzības slānim norāda mehānismu, segto apdraudējumu un tā ietekmes robežas. Mazs uzņēmums to uztur kā divu lappušu tabulu: kolonna aizsardzības slānis, kolonna apdraudējums no paša apdraudējumu modeļa, kolonna atlikušais risks. Pietiek ar savstarpēju atsauci uz SR-2 apdraudējumu modeli, saturs nav jāuztur divreiz.

◯ Atvērta ◯ Procesā ◯ Izpildīta ◯ Neattiecas

Pierādījums / pamatojums

SG-2 **Dokumentācija nosauc drošības pasākumus, ko produkts pats nenodrošina, bet sagaida no ieviešanas vides, piemēram, tīkla segmentāciju, priekšā esošus ugunsmūrus, fizisku piekļuves pārvaldību vai ārēju laika pakalpojumu, un skaidri norāda, ka bez šiem pasākumiem apliecinātais drošības līmenis netiek sasniegts.** Dokuments

Pēc kā to var atpazīt: Nodaļa rokasgrāmatā par ieviešanas priekšnosacījumiem vai atsauces arhitektūras zīmējums ar zonām un savienojumiem, kurā skaidri atzīmēti pasākumi, ko nodrošina aktīva īpašnieks. Praksē ir noderīgs saraksts ar pieņēmumiem par vidi, kas atvasināts tieši no produkta drošības konteksta un tiek pārlasīts katrai produkta versijai.

◯ Atvērta ◯ Procesā ◯ Izpildīta ◯ Neattiecas

Pierādījums / pamatojums

SG-3 **Pastāv drošas pamatkonfigurācijas rokasgrāmata, kas uzskaita visus drošībai nozīmīgos iestatījumus, pakalpojumus, portus un saskarnes, norāda ieteicamo piegādes stāvokli un apraksta novirzes no šī ieteikuma ietekmi.** Dokuments

Pēc kā to var atpazīt: Nostiprināšanas rokasgrāmata ar iestatījumu tabulu: parametrs, ieteicamā vērtība, ietekme, blakusparādība novirzes gadījumā. Papildus saraksts ar pakalpojumiem un portiem, kas ir aktīvi noklusējuma konfigurācijā, un pamatojums, kāpēc tie paliek ieslēgti. Maza komanda šo tabulu tur tieši blakus konfigurācijas failam repozitorijā un eksportē to piegādes dokumentācijā, tādēļ tā saglabā saskaņu ar produktu.

◯ Atvērta ◯ Procesā ◯ Izpildīta ◯ Neattiecas

Pierādījums / pamatojums

SG-4 **Pastāvīgai ekspluatācijai pastāv rokasgrāmata, kas apraksta, kā produkts tiek droši ekspluatēts, uzraudzīts un uzturēts drošā stāvoklī, tostarp rezerves kopijas un atjaunošana, žurnalēšana un rīcība ar drošībai nozīmīgiem notikumu ziņojumiem.** Dokuments

Pēc kā to var atpazīt: Ekspluatācijas rokasgrāmata ar sadaļām par žurnalēšanu, rezerves kopijām, restartēšanu un notikumu ziņojumiem. Kā papildu pierādījums saraksts ar drošībai nozīmīgiem ziņojumiem, ko produkts izdod, katram ar īsu ieteicamo rīcību, tādēļ aktīva īpašniekam tie nav jāinterpretē vienam pašam.

◯ Atvērta ◯ Procesā ◯ Izpildīta ◯ Neattiecas

Pierādījums / pamatojums

SG-5 **Dokumentācija skaidro, kā tiek izveidoti un uzturēti produkta lietotāju konti, lomas un atļaujas, jo īpaši lomu nodalīšana, noklusējuma piekļuves datu maiņa un vairs nevajadzīgu kontu dzēšana.** Dokuments

Pēc kā to var atpazīt: Nodaļa par kontu pārvaldību ar lomu pārskatu un katrai lomai piešķirtajām tiesībām, kā arī skaidra norāde par noklusējuma piekļuves datiem un to maiņu, nododot ekspluatācijā. Praksē labi darbojas īss nodošanas ekspluatācijā kontrolsaraksts rokasgrāmatā, ko aktīva īpašnieks var atzīmēt un saglabāt.

◯ Atvērta ◯ Procesā ◯ Izpildīta ◯ Neattiecas

Pierādījums / pamatojums

SG-6 **Pastāv rokasgrāmata drošai izņemšanai no ekspluatācijas, kas apraksta pilnīgu sensitīvu datu dzēšanu no produkta, piemēram, piekļuves datu, atslēgu, konfigurācijas datu un žurnālu, pirms ierīce tiek nodota tālāk, izmantota atkārtoti vai utilizēta.** Dokuments

Pēc kā to var atpazīt: Sadaļa par izņemšanu no ekspluatācijas, kurā uzskaitīta katra sensitīvu datu glabāšanas vieta produktā un atbilstošā dzēšanas procedūra, tostarp gadījumi, kad dzēšana tehniski nav iespējama un aparatūra ir fiziski jāiznīcina. Te palīdz pastāvīgo datu glabātuvju saraksts, kas ņemts no arhitektūras apraksta, jo tas neļauj kādu glabāšanas vietu aizmirst.

◯ Atvērta ◯ Procesā ◯ Izpildīta ◯ Neattiecas

Pierādījums / pamatojums

SG-7 **Lietotājiem piegādātā drošības dokumentācija pirms laidiena tiek pārskatīta: tā ir tehniski pareiza, saskanīga ar piegādāto produkta versiju, pilnīga attiecībā pret paredzēto saturu un saprotama paredzētajai auditorijai, un tā tiek atjaunināta ikreiz, kad mainās produkts.**

Pēc kā to var atpazīt: Pārskatīšanas ieraksts katram dokumentam un produkta versijai ar pārskatītāju, datumu, konstatējumiem un to slēgšanu, saistīts ar laidiena apstiprinājumu. Mazs uzņēmums to risina ar četru acu principu dokumentācijas izmaiņu pieprasījumā: viens izstrādātājs pārbauda tehnisko saturu, otra persona pārbauda saprotamību, un apstiprinājums tiek reģistrēts pieteikumā. Versija ir piegādājama tikai tad, kad pārskatīšana ir dokumentēta.

◯ Atvērta ◯ Procesā ◯ Izpildīta ◯ Neattiecas

Pierādījums / pamatojums