TLP:CLEAR

SEGURU TANBA DEZEÑU

MUDA EKUILÍBRIU RISKU SEGURANSA SIBERNÉTIKA:

PRINSIPIU NO APROXIMASAUN BA SEGURU HO SOFTWARE DEZEÑU

TLP:CLEAR

Communications Security Establishment

Canadian Centre for Cyber Security

Centre de la sécurité des télécommunications

Centre canadien pour la cybersécurité

Konteúdu

VIZAUN JERÁL: VULNERAVÊL TANBA DEZEÑU

Teknolojia integradu ba kuaze hotu-hotu faseta moris loroloron nian, ho aumenta barak sistema ne'ebé liga internet no liga ita hotu ba sistema krítiku ho impaktu direktu ba ami-nia prosperidade ekonómika, meius subsistênsia no to'o saúde, desde jestaun identidade pesoal to'o kuidadu médiku. Ezemplu desadvantajen ida husi konveniênsia sira mak violasaun sibernétika global ho rezulta kansela sirurjia ospital sira no diverte kuidadu ba pasiente sira. Teknolojia la seguru no vulnerabilidade sira iha sistema kritikál bele konvida invasaun sibernétika malisiozu ne'ebé bele hamosu risku seguransa[1] potensiál.

Nu'udar rezultadu ida, krusiál duni ba fabrikante software sira halo seguru liuhosi dezeñu no seguransa tanba padraun sira sai pontu fokal husi dezeñu produtu no prosesu dezenvolvimentu sira. Forsenedór balun halo ona progresu boot ba avansadu industria iha garantia software, enkuantu sira seluk kontinua atrazadu. Organizasaun autora enkoraja tebes kada fabrikante teknolojia atu konstrui sira-nia produtu bazeia ba redus karga seguransa ne'ebé kliente sira tenke simu, inklui prevene sira husi obrigasaun beibeik hala'o monitorazasaun, atualizasaun rotina no kontrola defeitu iha sira-nia sistema atu mitiga intrusaun sibernétika. Ami mós alerta fabrikante software sira ba konstrui sira produtu ho meius ne'ebé fasilita automasaun konfigurasaun, monitoramentu no atualizasaun rotina. Enkoraja ona ba fabrikante sira asumi responsabilidade atu melloria rezultadu seguransa husi sira-nia kliente hirak. Istorikamente, fabrikante software sira konfia ba hadi'ak vulnerabilidade ne'ebé hetan depois kliente sira implanta produtu sira, presija kliente sira ba implementa patches ho sira-nia osan rasik. Só deit ho inkorpora prátika seguru tanba dezeñu, Ita sei bele hakotu siklu visiozu husi kriasaun no aplikasaun koresaun beibeik ka konstante. **Nota:** Termu "seguru tanba dezeñu" inklui rua hotu seguru tanba dezeñu no seguru tanba padraun.

Atu atinji altu padraun seguransa software ida ne'e, organizasaun autora sira seluk enkoraja fabrikante sira prioritiza integrasaun seguransa produtu nu'udar pré-rekuisitu krítiku ba rekursu no velosidade lansamentu ba merkadu. Hamutuk ho tempu la'o hela, ekipa enjeñariu sei bele estabelese ritmu estável foun iha ne'ebé seguransa dezeña no hamenus esforsu atu mantidu tebes.

Reflete ba perspektivu ida ne'e, Uniaun Europeia reforsa importânsia ba seguransa produtu iha Lei Reziliensia Sibernétika, enfaze katak fabrikante sira tenke implementa seguransa durante siklu vida tomak produtu, hodi evita fabrikante sira husi introdus produtu vulnerável tama ba merkadu.

[1] Organizasaun autora sira rekoñese katak termu "seguransa" iha signikamentu barak depende ba kontekstu uza nia. Ba objetivu husi guia ida ne'e, "seguransa" sei refere ba aumenta padraun seguransa teknológika atu proteje kliente sira kontra atividade sibernétika malisioza hirak.

Atu kria futuru ida ne'ebé teknolojia no produtu asosiadu seguru liutan ba kliente sira, organizasaun autor insentiva fabrikante sira atu renova sira-nia dezeñu no programa dezenvolvimentu sira atu permite deit manda produtu seguru tanba dezeñu no tanba padraun. Kleur molok dezenvolvimentu, produtu sira ne'ebé seguru tanba dezeñu ne'e konseptualiza ho seguransa kliente nu'udar objetivu negosiu prinsipál, laos deit rekursu tékniku. Produtu seguru tanba dezeñu inisiu ho objetivu ida ne'eba molok komesa dezenvolvimentu. Produtu ezistente bele evolui ba estadu seguru tanba dezeñu liuhusi múltipla iterasaun. Produtu seguru tanba padraun mak sira ne'ebé seguru atu uza "ho kreativu" ho ladun barak mudansa ka altera konfigurasaun ka lalika altera ida, no rekursu seguransa disponivel sein kusta adisionál. Hamutuk, filosofia rua sira ne'e hasai barak ona todan atu mantein seguru ba fabrikante sira no redus oportunidade ne'ebé kliente sira sei sai vitima ba insidente seguransa rezulta husi konfigurasaun sala, koresaun kliente sira insufisientemente lalais ka problema komun sira seluk.

Ajênsia Seguransa Sibernétika no Infraestrutura (CISA), Ajênsia Seguransa Nasional (NSA), Departamentu Federal Investigasaun (FBI) no parseiru internasional hirak tuir mai ne'e[2] fornese rekomendasaun sira iha guia ida ne'e nu'udar roteiru ida ba fabrikante software sira garante seguransa ba sira-nia produtu:

- Sentru Australianu Seguransa Sibernétika (ACSC)
- Sentru Kanadense Seguransa Sibernétika (CCCS)
- Sentru Nasional Seguransa Sibernétika Reinu Unidu (UK)
- Eskritóriu Federal Seguransa Informasaun Alemanha (BSI)
- Sentru Nasional Seguransa Sibernétika Ólanda
- Sentro Nasional Seguransa Sibernétika Noruega (NCSC-NO)
- Ekipa Resposta Emerjênsia Informática Nova Zelândia (CERT NZ) no Sentru Nasional Seguransa Sibernétika Nova Zelândia (NCSC-NZ)
- Ajênsia Koreana Internet no Seguransa (KISA)
- Diresaun Nasional Sibernétika Israel (INCD)
- Sentru Nasional Preparasaun no Estratéjia husi Insidente ba Seguransa Sibernétika (NISC) Japaun no Sentru Koordenasaun Ekipa Resposta Emerjênsia Informática Japaun (JPCERT/CC)
- Rede OEA/CICTE Ekipa Resposta Insidente Sibernétika Governamental (CSIRT) Amérika
- Ajênsia Seguransa Sibernétika Singapura (CSA)
- Ajênsia Nasional Seguransa Sibernétika no Informasaun República Tcheca (NÚKIB)

Organizasaun autora sira rekoñese kontribuisaun husi parseiru sektor privadu barak iha avansu seguru tanba dezeñu no seguransa tanba padraun. Produtu ida ne'e destinadu atu promove diálogu internasional kona-ba prinsipal prioridade sira, investimentu no dezisaun nesessáriu atu alkanse futuru ida ne'ebé teknolojia seguru, proteje no reziliente tanba dezeñu no padraun. Ba ida ne'e, organizasaun autora sira ba buka feedback husi parte interessadu sira kona-ba produtu ida ne'e no intende atu konvoka série sesaun audisaun hirak atu refina liutan, espesifika np avansa ami-nia orientasaun atu alkanse ami-nia objetivu komun.

Atu obten informasaun kona-ba importânsia seguransa produtu, hare artigu CISA, Impaktu husi Teknolojia La Seguru no Sa'ida Ita Bele Halo Kona-ba Ida ne'e.

[2] Depois husi ne'e denominadu nu'udar "organizasaun autora".

SA'IDA MAK FOUN

Publikasaun inisial husi relatóriu ida ne'e jera kuantidade signifikativa ida ba konversa iha indústria software laran. Notísia diária husi organizasaun no indivídu sai destaka kompromete ba nesesidade konversa liutan kona-ba oinsá rezolve problema krôniku no sistêmiku iha produtu software laran.

Depois lansamentu iha Abril 2023, organizasaun autoras (depois husi ne'e denominadu nu'udar "ami" no "ami nia") simu feedback atensiozu atus ba atus husi indivídu, empreza no asosiasaun komersial sira. Solisitasaun ida ne'ebé komun liu iha feedback ne'e mak fornese detalle liutan kona-ba prinsípiu tolu apliká ba fabrikante software no sira-nia kliente. Iha dokumentu ida ne'e, ami espande relatóriu orijinal no aborda tema sira seluk hanesan tamañu fabrikante no kliente, maturidade kliente nian no eskopu prinsípiu sira.

Software ne'e mak iha fatin hotu-hotu no la iha relatóriu ida sei bele kobre adekuadamente sistema software hotu, dezenvolvimentu ba produtu software, implantasaun no manutensaun no integrasaun ho sistema sira seluk. Ba orientasaun iha kraik ne'e ne'ebé la klaru mapeia ba ambiente espesífiku, ami sei espera atu rona husi komunidade kona-ba oinsá prátika sira esplika iha dokumentu ida ne'e kauza melloria seguransa espesífikamente.

Relatóriu ida ne'e aplika ba fabrikante sistema no mós modelu software intelijênsia artifisial (IA) sira. Embora sira iha diferensa husi forma tradisional software, prátika fundamental seguransa nafatin aplika ba sistema no modelu IA nian. Balun husi prátika seguru tanba dezeñu sei presija modifikasaun atu tenta konsiderasaun espesífika ba IA, mais prinsípiu jeral tolu ba seguransa tanba dezeñu aplika ba sistema IA hotu-hotu.

Ami rekoñese katak transforma siklu vida dezenvolvimentu software (SDLC) para se aliña ho prinsípiu seguru tanba dezeñu sira ne'e laos tarefa simples ida no sei han tempu. Aléinde, fabrikante software kiik sira sei araska atu implementa sujestaun barak sira ne'e. Ami fiar katak industria software tenke disponivel luan tan ekipamentu no prosidementu sira ne'ebé halo produtu sira seguru liutan. Tanba aumenta barak ema no organizasaun sira konsentra sira-nia atensaun ba melloria seguransa software, ami fiar iha espasu ba inovasaun ne'ebé sei redus distânsia entre fabrikante boot no kiik sira ba kliente sira hotu nian benefísiu.

Atualizasaun ida ne'e ba relatóriu orijinal seguransa tanba dezeñu ne'e mak parte husi ami-ni kompromisu atu kontstrui parseria ho komunidade interkonektadu husi parte interesadu barak liutan mak sustenta ami-nia ekosistema teknológiku. Ida ne'e rezultadu feedback husi parte barak ekosistema ida ne'eba, no ami sei kontinua ba rona no aprende husi perspektivu sira. Maski dezafia barak iha futuru, ami optimistiku tebes tanba ami aprende liutan kona-ba ema no organizasaun sira ne'ebé adota ona filosofia seguru tanba dezeñu, kada vez ho susesu.

OINSÁ ATU UZA DOKUMENTU IDA NE'E

Ami obriga fabrikante software sira ba adere prinsípiu sira iha dokumentu laran ida ne'e. Fabrikante software sira bele demonstra sira-nai kompromisu ho dokumentadu publikamente sira-nia asaun mak foti ona, akordu ho etapa hirak ne'ebé lista iha kraik ne'e. Ami enkoraja fabrikante software sira ba buka tátika hirak mak kompletu espíritu prinsípiu ida ne'e no atu kria artefatu sira ne'ebé sei konstrui argumentu interese to'o ba kliente ohin nian no kliente potensial sira mak sente ladun fiar, katak sira inkorpora filosofia seguransa tanba dezeñu.

Aléinde ba asaun sira mak tenke foti husi fabrikante software sira, kliente mós bele aproveita dokumentu ida ne'e. Empreza sosa software tenke husu pergunta difísil sira ba sira-nia fornesedór, ho foti inspira husi ezemplu adesaun ba prinsípius sira mak lista ona iha dokumentu ida ne'e. Ho halo ida ne'e, kliente sira bele ajuda ba muda merkadu hasoru produtu sira ne'ebé seguru liutan tanba dezeñu. Ezemplu ida husi pergunta kliente sira nian bele husu fornesedór ne'e mak fornese iha Guia CISA ba Akuizisaun Teknolojia K-12.

Ami enkoraja kliente emprezal sira ba inkorpora prátika sira ne'e tama ba prosesu akuizisaun, avaliasaun due diligence fornesedór sira, dezisaun aseitasaun risku emprezal no etapa sira seluk mak foti ona kuandu avalia fornesedór sira. Kliente sira mós tenke enkoraja fornesedór sira ba dokumentu publikamente asaun seguru tanba dezeñu ne'ebé sira foti ona. Koletivamente, ida ne'e bele kria sinal forte ba seguransa, ne'ebé bele enkoraja no permite fabrikante software sira foti etapa hirak ba seguransa boot liutan. Ho lian seluk, hanesan ita ba buka atu kria filosofia seguransa tanba dezeñu difundida entre fabrikante software sira, ami presija kria kultura "seguransa tanba demanda" ho sira-nia kliente hirak.

Seguru tanba Dezeñu

"Seguru tanba Dezeñu" signifika katak produtu teknolojia sira konstrui iha meius ne'ebé proteje makas kontra atór sibernétika malisiozu sira ho susesu obten asesu ba dispositivu sira, dadus no infraestrutura ligadu. Fabrikante software sira tenke realiza avaliasaun risku atu identifika no enumera ameasa sibernétika sira ba sistema krítiku no depois inklui protesaun iha modelu produtou sira ne'ebé responsabiliza ba senáriu ameasa sibernétika mak evolusaun.

Prátika seguru dezenvolvimentu teknolojia informasaun (TI) no múltipla kamada defeza – koñesidu nu'udar defeza profunda – ne'e mós rekomenda atu evita ator malisiozu sira husi kompremete sistema ka obten asesu naun autorizadu ba dadus konfidensial. Organizasaun autora depois rekomenda ba fabrikante sira uza modelu ameasa mak personaliza durante etapa dezenvolvimentu produtu atu rezolve ameasa potensial hotu-hotu ba sistema no konta ba kada prosesu implantasaun sistema.

Organizasaun autora obriga fabrikante sira ba adota abordajen seguransa olístika ba sira-nia produtu no plataforma sira. Dezenvolvimentu seguru tanba dezeñu presija investimentu estratéjiku husi rekursu dedikadu ho fabrikante software sira iha kada kamada husi dezeñu produtu no prosesu dezenvolvimentu ne'ebé labele "aparafuzadu" iha futuru. Presija lideransa forte husi parte ezekutivu negósiu prinsipal fabrikante nian atu halo seguransa nu'udar prioridade komersial, laos deit karakterística téknika. Kolaborasaun ida ne'e entre lider negósiu no ekipa téknika sira estende husi etapa preliminariu husi dezeñu no dezenvolvimentu, liuhusi implementasaun no manutensaun kliente nian. Enkoraja fabrikante sira atu halo kompenzasaun enduresimentu no investimentu sira inklui sira ne'ebé "invisível" ba kliente sira (p.e., migrasaun ba lingua programa ne'ebé elimina vulnerabilidade jeneralizadu). Sira tenke prioritiza rekursu, mekanizmu no implementasaun ekipamentu sira ne'ebé proteje kliente sira duke rekursu produtu ho parese atrai, mais aumenta superfísie atake.

La iha solusaun úniku atu hakotu ameasa persistente husi ajente sibernétika malisiozu ba esplora vulnerabilidade teknológika no produtu sira ne'ebé "seguru tanba dezeñu" sei kontinua sofre vulnerabilidade; entantu, vulnerabilidade barak kauza tanba ninia problema báziku. Fabrikante sira tenke dezenvolve roteiru eskrita atu aliña sira-nia modelu produtu mak eziste ona ho prátika dezeñu seguru liutan, garante halo desviu deit iha situasaun eksepsional.

Organizasaun autora rekoñese katak asumi propriedade rezultadu seguransai ba kliente sira no garante nivel seguransa kliente ida ne'e sei aumenta kusta dezenvolvimentu. Entantu, investe iha prátika seguru tanba dezeñu, mezmu dezenvolve produtu teknolójiku inovador sira no manten sira mak eziste ona bele melloria substansialmente postura seguransa kliente sira no redus probabilidade komprometimentu. Prinsípiu seguransa tanba dezeñu laos deit fortalese postura seguransa ba kliente sira no reputasaun marka ba desenvolvedor sira, mais prátika mós redus kusta manutensaun no patches ba fabrikante sira iha prazu naruk.

Sesaun Rekomendasaun ba Fabrikante Software lista ona iha kraik ne'e fornese lista prátika no polítika dezenvolvimentu produtu ba fabrikante sira atu konsidera.

Seguru tanba Padraun

"Seguru tanba padraun" signifika katak produtu sira ne'e reziliente kontra téknika esplorasaun predominante no prontu atu uza sein kustu adisional. Produtu sira ne'e proteje kontra ameasa vulnerabilidade prevalente duni sein uzuáriu final tenke foti etapa adisional atu proteje sira. Produtu seguru tanba padraun ne'e dezeñu ona atu halo kliente sira konsiente katak kuandu sira desvia husi padraun seguru, sira aumenta posibilidade kompremetidu só deit sira implementa kontrola kompensatóriu adisional. Seguru tanba padraun ne'e mak forma husi seguru tanba dezeñu.

- Konfigurasaun ida seguru tenke sai liña baze padraun nian. Produtu seguru tanba padraun automatikamente ativa kontrola seguransa importante liu presija atu proteje empreza kontra ator sibernétiku maliziosu sira, no mós fornese kapasidade atu uza no konfigura seguransa liutan ho sein kustu adisional.
- Kompleksidade husi konfigurasaun seguransa labele sai problema kliente nian. Ekipa TI organizasional frekuentemente karega demais ho responsabilidade operasional no seguransa, rezulta iha tempu limitadu ba komprende no implementa implikasaun no mitigasaun seguransa mak presija ba postura robusta seguransa sibernétika. Fabrikante sira bele ajuda sira-nia kliente ho otimiza konfigurasaun segura produtu – proteje "kamiñu padraun" – garante sira-nia produtu fabrika ona, distribuí no uza seguru akordu ho padraun "seguru tanba padraun".

Fabrikante sira husi produtu mak "seguru tanba padraun" la fó kusta estra ba implementa konfigurasaun seguransa adisional. Kontrariu, sira inklui tama ba produtu báziku, hanesan sintu seguransa mak inklui iha kareta foun hotu-hotu.

Seguransa la bele sai opsaun luxu, maibe tenke konsidera nu'udar direitu kliente sira tenke simu sein iha negosia ka selu liutan.

REKOMENDASAUN BA FABRIKANTE SOFTWARE SIRA

Guia konjuntu ida ne'e fornese rekomendasaun sira ba fabrikante atu dezenvolve roteiru eskrita atu implementa no garante seguransa TI nian. Organizasaun autora sira rekomenda fabrikante software sira implementa estratejia ne'ebé esplika iha seksaun kraik ne'e atu asumi propriedade husi rezultadu seguransa sira-nia kliente liuhusi prinsipiu seguru tanba dezeñu no padraun.

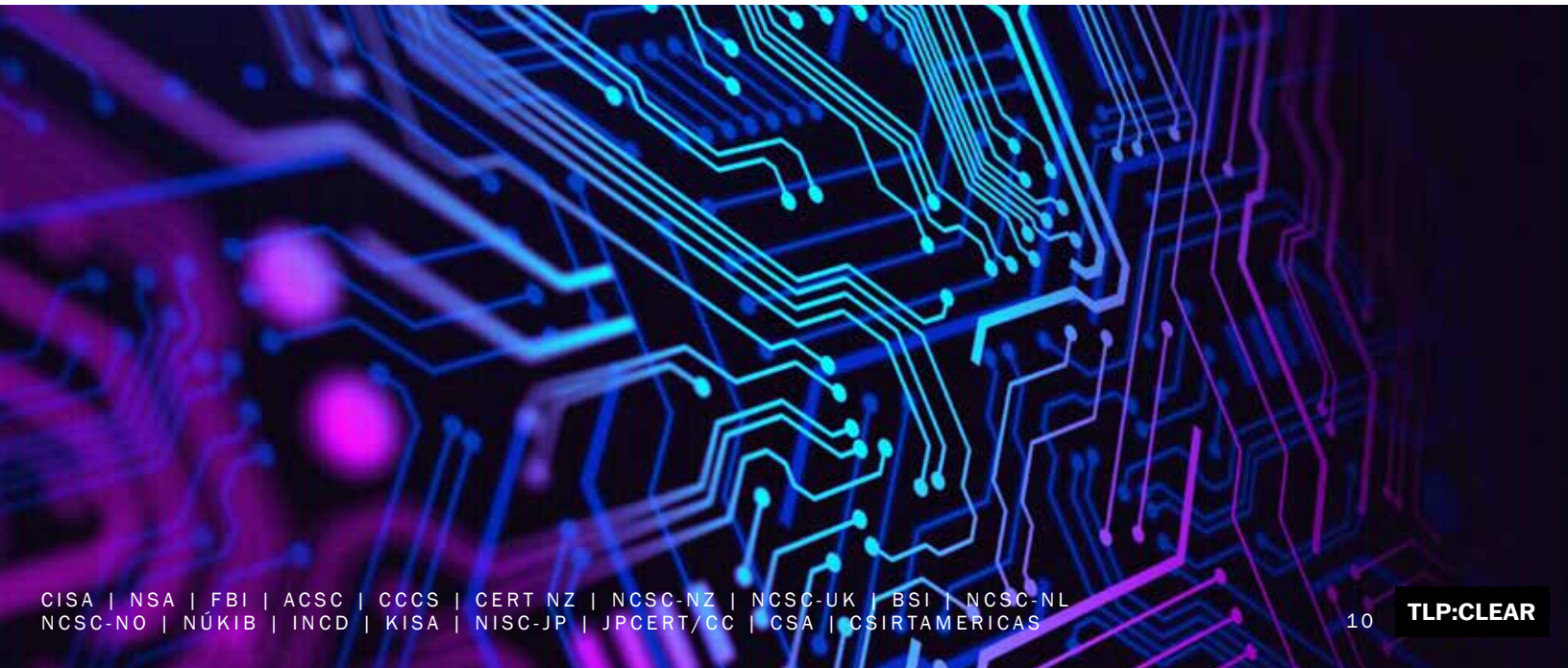
PRINSÍPIU SEGURANSA PRODUTU SOFTWARE SIRA

Fabrikante software sira enkoraja ba adota foku estratejia ida ne'ebé prioritiza seguransa software nian. Organizasaun autora sira dezenvolve prinsipiu prinsipál tolu sira ne'e atu orienta fabrikante software sira ba konstrui seguransa software tama ba sira-nia prosesu dezeñu molok dezenvole, konfigura no enviu sira-nia produtu.

1 **Asumi propriedade ba kontrola seguransa kliente** no dezenvolve produtu sira akordu ida ne'e. Karga seguransa laos kliente mesak deit mak lori ninia todan.

2 **Adota transparênsia no responsabilidade radikal.**
Fabrikante software sira tenke orgullu ba sira-nia aan iha fornese produtu seguru no proteje, no mós diferensa sira-nia aan husi komunidade fabrikante sira seluk bazeia ba sira-nia kapasidade atu halo hanesan ne'e. Ida ne'e bele inklui fahe informasaun sira aprende ona husi implantasaun sira-nia kliente, hanesan uza mekanizmu autentikasaun forte liuhusi padraun. Ne'e mós inklui kompromisu forte atu garante avizu kona-ba vulnerabilidade no nota rejistu vulnerabilidade komun no espozisaun (CVE) kompletu ona no akuradu. Entantu, kuidadu ho tentasaun ba konta CVEs nu'udar métrika negativa, tanba númeru sira ne'e mós sinal ba komunidade saudável análize no teste kódigu.

3 **Konstrui estrutura organizasional no lideransa atu alkanse objetivu sira ne'e.**
Embora koñesimentu tékniku kritikal ba seguransa produtu, ezekutivu senior sira mak tomadór dezisaun prinsipal atu implementa mudansa iha organizasaun ida. Ezekutivu tenke prioritiza seguransa nu'udar elementu kritikal ba dezenvolvimentu produtu iha organizasaun tomak no iha parseiramentu ho kliente sira.



Atu ativa prinsípiu tolu sira ne'e, fabrikante sira tenke konsidera tátika operasional balun atu evolui sira-nia prosesu dezenvolvimentu.

Konvoka reuniaun rotina ho lideransa ezekutivu empreza sira atu enfaze importânsia seguransa tanba dezeñu no seguransa tanba padraun iha organizasaun laran. Polítika no prosedimentu tenke estabelese atu rekompensa ekipa produsaun ne'ebé dezenvolve produtu kumpri ba prinsípiu sira ne'e, ne'ebé bele inklui prémiu tanba implementasaun prátika seguransa di'ak tebes ka insentivu ba nivel empregu no kritériu promosaun.

Opera bazeia ba importânsia seguransa software ba susesu negósiu. Por ezemplu, konsidera nomeia "líder seguransa software" ka "ekipa seguransa software" ne'ebé defende prátika komersial no TI mak diretamente liga padraun seguransa software no responsabilidade fabrikante nian. Fabrikante sira tenke garante katak sira iha robusta, avaliasaun seguransa produtu independente no programa avaliasau ba sira-nia produtu.

Uza modelu ameasa personalizadu durante alokasaun no dezenvolvimentu rekursu para prioritiza rekursu krítiku no ho altu impaktu. Modelu ameasa konsidera kazu uza produtu espesifika ida no ekipa dezenvolvimentu bele fortifika produtu sira. Finalmente, lideransa sênior tenke responsabiliza ba ekipa atu fornese produtu seguru sira nu'udar elementu prinsipal ba superioridade no kualidade produtu nian.

Nu'udar parte husi atualizasaun Outubru 2023 ba guia ida ne'e, prinsipiu tolu sira ne'e mak espande liuhosi esplikasaun tuir mai, demonstrasaun no evidensia.

PRINSÍPIU 1: Asumi propriedade Rezultadu Seguransa Kliente nian

ESPLIKASAUN

Prátika ida melloria mak rekomenda ne'ebé fabrikante software sira investe iha esforsu seguransa produtu mak inklui **refosa aplikativu, rekursu aplikativu sira,** no konfigurasaun padraun **aplikativu.**

Fabrikante software sira tenke implementa **protesaun ba aplikativu** ho uza prosesu no teknolojia sira ne'ebé levanta kustu ba atór melisiozu ida mak intende atu kompromete aplikativu sira. Prosidementu no protokolu protesaun aplikativu ajuda rezistente produtu sira hetan atake husi atór malisiozu matenek sira. Termu hanesan afrouximentu, seguransa produtu no reziliente sira ne'e hotu-hotu relasiona besik ba kualidade produtu nian. Ideia ne'e katak seguransa tenke "inkorpora" no laos "apafuzadu." [1] Ho inkorpora iha seguransa, fabrikante software sira labele aumenta seguransa kliente nian maibe mós aumenta sira-nia produtu kualidade. Ezemplu tátika inklui garante entrada uzuáriu nian ne'e validu no ijiene, no laos hatama diretamente ba kódigu laran (p.e, uza konsulta parametrizadu), uza lingua programasaun seguru memória ida, jerensiamentu rigorosu siklu vida dezenvolvimentu software (SDLC) no uza hardware-jerensiamentu xave kriptográfika apoiu.

Aplikativu sira tenke apoiu **rekursu aplikativu sira** ne'ebé relasiona ho seguransa síbernetika. Dalaruma hanaran "abilidade," rekursu sira ne'e estende funsionalidade

husi produtu ka servisu ida iha maneira ne'ebé ajuda mantein ka aumenta postura seguransa husi kliente ida. Ezemplu rekursu sira relasiona ho seguransa inklui suporte seguransa xamada transporte (TLS) ba koneksaun sira hotu, suporta logon úniku (SSO), suporta autentikasaun multifator (MFA), rejistru auditoria eventu seguransa sira, kontrola asesu bazeia ba funsaun (RBAC) no kontrola asesu bazeia ba atributu (ABAC).

Balun husi rekursu produtu sira ne'e konfigurável, permite kliente sira atu integra produtu fasil liutan tama ba sira-nia ambiente ezistente ona no flutua traballu sira. Konfigurasaun sira ne'e signifika ba aplikativu sira tenke iha **konfigurasaun padraun** define to'o kliente konfigura sira. Konfigurasaun padraun sira ne'e tenke konfigura seguru "prontu atu uza" entaun kliente espende rekursu oituan atu halo sira-nia kompilasaun produtu teknolojia seguru liutan.

Kada elementu sira ne'e – protesaun/afrouximentu aplikativu, rekursu seguransa aplikativu no konfigurasaun padraun aplikativu – kaer papél iha seguransa aplikativu nian no rezultante postura seguransa husi kliente. Fabrikante software sira tenke hanoin kona-ba kada elementu sira ne'e no oinsá sira konekta ba malu. Fabrikante sira tenke hanoin kona-ba liutan duke sira-nia investimentu deit atu inkorpora elementu sira ne'e tama ba sira-nia produtu. Fabrikante sira tenke foti etapa liutan no konsidera hanusa elementu sira muda postura seguransa sira-nia kliente, ba di'ak liutan ka aumenta aat liutan.

Fabrikante sira tenke asumi propriedade seguransa sira-nia klienta duke sukat sira-nia aan prinsipalmente ba sira-nia esforsu no investimentu. Responsabilidade tenke koloka montante, ho fabrikante sira, iha ne'ebé iha probilidade boot redus posibilidade ba kompromisu.

Infelizmente, kazu ne'e laos hanesan ne'e ohin loron. Barak fabrikante koloka sira-nia karga seguransa ba kliente duke investe ba fortifika komprehensivu **seguransa aplikativu.** Por ezemplu, kuandu fabrikante korije vulnerabilidade ida, ami sempre hare vulnerabilidade hanesan esposta tanba sira rezolve sintomas duke kauza prinsipal husi defeitu. Produtu bele implementa mitigasaun diferente iha várias parte husi baze kódigu ba klasse vulnerabilidade hanesan. Nu'udar kazu ba pontu ne'e, depois fabrikante korijiu vulnerabilidade sanitizasaun entrada, peskizadór sira ka invasór sira hetan trajetu kódigu ne'ebé la fó benefisiu husi sanitizasaun entrada aprimoradu. Fabrikante aplika koresaun sira iha tempu ida duke unifika baze kódigu atu elimina klasse vulnerabilidade ne'eba iha aplikativu tomak.

Rekursu aplikasaun sira bele kria tantu benefisiu no risku ba kliente sira. Rekursu sira ne'ebé permite pontu integrasaun sira ho sistema no versaun barak bele aumenta boot valór produtu ida. Entantu, rekursu suporta sein planu apozentadór, hanesan protokolu rede, bele husik vulnerabilidade kliente nian karik sira menus komprensaun husi implikasaun ba uza kontinua rekursu ida ne'eba. Por ezemplu, produtu balun kontinua uza protokolu rede ne'ebé iha sira-nia orijen iha dékada 1990 ka 2000 no koñese hanesan la seguru. Iha váriu fatór sira ne'ebé bele halo neineik ba kliente-nia rapidu atu atualiza no implementa medidas seguransa modernu. Sira bele uza produtu hirak ne'ebé integra ho rede organizasaun restu, maibe menus medidas seguransa modernu, prevene ekipa TI husi modernizasaun. Nafatin, fabrikante software sira bele hatama padraun sira ne'e ba sira-nia prosesu planemantu atu enkoraja kliente sira manten atualizadu.

Konfigurasaun padraun aplikativu ne'e mak areia adisaun husi risku potensial ba kliente sira. Fabrikante sira sempre hili konfigurasaun padraun ida, halo fasil liutan ba kliente sira atu uza rekursu aplikativu mak sira hakarak. Desvantajen ne'e katak prátika ida ne'e aumenta atake superfísie ba kliente sira ne'ebé karik la presija rekursu no protokolu balun mak abilita ho padraun. Aléinde, barak kontrola seguransa desativadu ho padraun ka presija kliente sira uza tempu atu konfigura sira-nia konfigurasaun atu aumenta seguransa. Modelajen ameasa eksplisita ne'e mak tátika ida ne'ebé bele ajuda informa dezisaun ida ne'ebé tenke ativadu ho padraun ka konfigurasaun ida ne'ebé mak presija atu seguru ho padraun. Tátika seluk ne'e mak atu investiga medidas sira atu halo rekursu bele detekta ba administradór.

Fabrikante balun enviadu produtu sira ho padraun ne'ebé bele kria risku ba sira-nia kliente balun ka hotu-hotu. Duke define padraun seguru liutan, sira sempre hili atu produs mais **guia afrouximentu** ne'ebé kliente sira tenke implementa ho kusta rasik. Guia afrouximentu sofre problema hirak ne'ebé komun. Guia afrouximentu balun araska atu ba buka no la suporta ho di'ak. Sira seluk komplikadu atu implementa, okazionalmentu presija dezenvolvimentu software atu eskrita modulu estensaun nian. Alende, sira mós hanoin katak leitór iha esperiênsia boot kona-ba seguransa sibernétika hodi komprende maneira husi konfigurasaun ida ne'ebé mak muda ona superfísie atake. Pratikante sira ne'ebé iha komprensaun la kompletu ba medidas ida ne'ebé invasór sira-nia traballu bele falla atu implementa instrusaun guia afrouximentu ho apropriu, espesialmente karik instrusaun la halo klaru ninia trade-off. Aléinde, laos guia afrouximentu hotu-htou eskrita ho enjeñeiru sira ne'ebé intimamente familiar ho tátika no ekonomia invasór nian, halo sira ba kria guia afrouximentu ne'ebé inefikas, mesmu implementa ho los ona. Rihun ba rihun kliente asumi responsabilidade atu proteje múltipla instânsia software ka sistema sira, dalaruma iha ambiente ho rekursu limitadu. Depende ba guia afrouximentu deit la ajuda ida.

Konfigurasaun aplikativu tenke avalia beibeik karik konfigurasaun ne'e padraun nian ka konfigura ho kliente, kontra komprensaun fabrikante atual nian kona-ba senáriu ameasa. Aplikativu sira tenke halo indikadór klaru kona-ba risku potensial ne'ebé bele rezulta husi konfigurasaun sira ne'eba no tenke halo indikadór sira ne'eba koñesidu. Hanesan karreta modernu deit iha indikadór kona-ba sintu seguransa no espresa katak indikadór ho halo lian alerta karik Ita tenta atu diriji sein uza sintu seguransa, sotfware tenke espresa indikadór sira kona-ba kondisaun sistema seguransa. Karik aplikativu ida konfigura ona la presija MFA ba konta administradór, nia tenke halo administradór regularmente siente katak sira no sira-nia organizasaun tomak iha perigu hela karik sira la konfigura MFA. Aléinde, karik aplikativu ida konfigura ona atu apoiu protokolu tuan nian ne'ebé agora koñese ona atu implementa kriptografia fraku, nia tenke regularmente halo klaru ba administradór katak organizasaun iha perigu laran no fornese rekursu sira atu rezolve situasaun ne'e. Ami urjente fabrikante sira atu implementa estímulu rotina ne'ebé konstrui tama ba produtu laran duke depende deit ba administradór atu halo tempu, esperiênsia no konsiente atu tradus guia afrouximentu sira. Oportunidade sira klaru duni eziste ba inovasaun atu balansu konsiderasaun seguransa no utilizasaun.

Kada elementu iha leten ne'eba kria situasaun insustentável iha ne'ebé kliente sira tenke halo peskiza, finansa, sosa, funsinairu, implanta no monitoriza **produtu seguransa** adisional atu redus oportunidade kompromisu. Organizasaun kiik no médiu (SMOs) jeralmente la bele fasilita opsaun sira ne'e. Sira infrenta falta iha koñesimentu, finanseiru, no tempu ne'ebé fó todan ba bandwith no funsaun, forsa seguransa ba prioridade abaixu no aumenta aat risku koletivu tomak. Resiprokamente, investimentu seguransa ho fabrikante balun relativu sei aumenta. Fraze komun ne'ebé rezumu problema ne'e katak indústria software presija produtu seguru liutan, laos produtu seguransa liutan. Fabrikante software sira tenke lidera transformasaun ne'e.

> ***Industria software presija produtu seguru liutan, laos seguransa produtu liutan. Fabrikante software sira tenke lidera transformasaun ne'e.***

Ohin loron, kadavez ami lee komentáriu husi fabrikante sira esplika katak kliente ida kompremete tanba labele ativu rekursu seguransa espesifiku ka halo tuir guia afrouximentu espesifiku. Aleinde, depois kompromisu ida, fabrikante sira tenke esplika karik rekursu seguransa espesifiku ida ka guia afrouximentu espesifiku ida sei prevene kompromisu no konsidera halo ida ne'e sai padraun ho sein kustu. Iha kazu sira ne'ebé produtu ne'e rasik la sufisiente proteje faze dezeñu no implementasaun, fabrikante tenke esplika oinsá sira esforsu atu elimina klasse vulnerabilidade husi sira-nia liña produtu.

Fabrikante software sira iha responsabilidade atu garante katak sira-nia produtu dezeñu no dezenvolve ona ho seguransa nu'udar prioridade prinsipal. Atu alkanse ida ne'e, sira tenke **sukat rezultadu objetivamente** ba sira-nia esforsu iha kampu ne'e. Ami apela ba fabrikante sira atu laos deit foku ba sira-nia esforsu internu, maibe ba medidas objetivamente no reportajen regularmente ba rezultadu no efikásia husi esforsu no konfigurasaun seguransa produtu, no atu konstrui siklu feedback ne'ebé kria mudansa iha SDLC ne'ebé lidera ba melloria mensurável iha seguransa do kliente no produtu seguru liutan. Relatóriu tenke inklui dadus anónimu ne'ebé komunidade akadémika no investigasaun seguransa bele uza atu akompaña tendênsias nivel altu no medida progresu ekosistema luan.

DEMONSTRA PRINSIPIU IDA NE'E

Fabrikante software no servisu online sira tenke ba buka medidas atu demonstra ho susesu ba implementa prinsipiu ida ne'e. Sira tenke ba buka atu fornese evidensia iha forma artefatu ba esterna sira atu ezamina. La iha artefatu ida ho ninia rasik sei prova katak fabrikante ida implementa hela robusta ho programa dezeñu, maibe ho fornese artefatu variu, sira sei konstrui kazu ida ba fabrikante-nia kompromisu atu dezenvolve produtu seguru. Abordajen ida ne'e iha espíritu husi "hatudu, duke konta deit".

Atu demonstra prinsipiu ida ne'e, fabrikante software sira tenke konsidera etapa hirak hanesan sira iha lista tuir mai. Organizasaun autora rekoñese katak fabrikante software balun sei bele implementa kedas pratika sira ne'e no produs artefatu korespondente iha inisiu husi sira-nia jornada seguru tanba dezeñu. Aléinde, fabrikante software sira sei presija atu prioritiza lista ida ne'e depende ba oinsá kliente sira implanta produtu iha kampu atu alkanse benefisiu seguransa boot liu.

PRÁTIKA SEGURU TANBA PADRAUN

1. **Elimina seña padraun.** Seña padraun kontinua ba implika tanba kauza husi atake oinoin kada tinan. Halo kompromisu atu elimina problema kroniku ida ne'e sei nega asesu fasil ba invasór sira. Mesmu, fabrikante sira tenke konsidera prátika seña sa'ida mak tenke implementa, hanesan seña ho naruk minimu no proibisaun ba seña koñese mak viola ona.

2. **Realiza teste kampu.** Ho teknolojia kontinua evolui no sai komplikadu liutan, ne'e aumenta importante ba fabrikante software sira atu realiza teste seguransa sentriku hodi komprende postura seguransa produtu sira nian iha kampu. Hanesan ho oinsá peskiza uzuáriu informa rekizitu dezenvolvimentu software, fabrikante software sira mós tenke konduz peskiza uzuáriu atu komprende iha ne'ebé esperiênsia uzuáriu (UX) seguransa insufisiente. Ho observa oinsá kliente sira implanta no uza sira-nia produtu iha ambiente real, fabrikante software bele obten opiniaun valór tama utilizasaun no efika husi sira-nia rekursu seguransa no kontrola. Opiniaun sira ne'e bele ajuda identifika area ba melloria no refinadu sira-nia produtu atu kompletu liutan nesesariu seguransa kliente nian. Por ezemplu, teste kampu bele sujere mudansa iha fluxu UX nian, padraun, alerta no monitoramentu. Teste kampu mós bele hatudu iha ne'ebé melloria pasadu ba dezeñu produtu redus velosidade husi seguransa pathces, redus erru konfigurasaun sira no minimiza superfísie atake.

Fabrikante sira tenke konsidera tuir mai ne'e:

- Kliente sira implementa guia afrouximentu koretamente ka?
- Rekursu seguransai ezitente iha produtu nian realiza nu'udar espera ona iha kampu ka?
- Rekursu sira ne'e rezistente loloos ka ba atake iha real?
- Rekursu ida ne'ebé di'ak liu redus posibilidade kompromisu?

Nota: Atu obten koñesimentu ba elementu sira ne'e, fabrikante software karik espera atu parseira ho kliente sira atu konduz ezersisiu ekipa mean hodi hare oinsá produtu reziste ba atake sira. Teste kampu sira ne'e bele realiza iha lokasaun fiziku kliente nian, virtualmente, ka liuhusi telemetria husi aplikativu iha maneira privadu.

3. **Redus tamañu guia afrouximentu.** Fabrikante sira bele hadi'ak postura seguransa kliente nian ho simplifikasaun ka elimina guia afrouximentu produtu nian no foku ba medidas seguransa kritikal prinsipal nian ne'ebé kliente sira tenke prioritiza kuanda implanta sira-nia produtu. Duke fó todan demais ba kliente sira ho lista medidas seguransa nian, fabrikante sira tenke identifika risku seguransa nivel altu ne'ebé sira-nia produtu suseitavel no fornese guia klaru no badak kona-ba oinsá atu mitiga risku sira ne'e. Entantu, fabrikante sira tenke fornese ba kliente sira ho ekipamentu no automatizasaun ne'ebé simplifika prosesu implementa kontrola seguransa nian, hanesan roteiru mak ho fasil bele implanta iha sira-nia ambiente. Aleinde, ekipamente sira ne'e bele verifika no klaramente hatudu mudansa mak halo ona husi baze liña orijinal nian. Ho simplifikasaun guia afrouximentu no fornese ba kliente sira ho ekipamentu no automatizasaun simples atu uza, fabrikante sira redus karga ba sira-nia kliente no ajuda garante katak sira-nia produtu implanta ona iha maneira seguru. Tátika ida ne'e mak atu konsidera implementa prinsípiu de Pareto hodi redus númeru ka etapa sira ba kazu uza komun sira (ida mak 80%) no, depois fornese orientasaun kontekstual no ekipamentu ba senáriu sira mak ladun komun (ho 20%). Iha medidas ida ne'e, fabrikante software sira sei halo buat simples sira no buat araska sira sai simples liutan se posivel.

Teste kampu sei sai ekipamentu ho poder ba sukat to'o bainhira kliente bele deskobre, komprende no implementa guia afrouximentu sira. Fabrikante sira tenke konsidera oinsá produtu tenke enkoraja administradór atu foti asaun ho produtu ne'e rasik duke depende deit ba sira atu implementa tarefa husi guia afrouximentu.

4. **Ativamente dezenkoraja uza rekursu legadu inseguru.**
Prioritiza seguransa liuhusi trajetu atualizasaun klaru kompara ho kompatibilidade antesedente nian. Publika postajen blog mak hatudu adosaun rekursu no protokolu seguru liutan, no dezkontinua rekursu la seguru ho anúnsiu, posivelmente husi produtu ne'e rasik. Númeru signifikativu husi kliente mak demonstra ona katak sira la mantein sira-nia sistema atual ho rede modernu, identidade no rekursu seguransa kritikal sira seluk. Iha kazu balun, kliente sira tauk ba funsionalidade mak iha bele sai aat ho atualizasaun ida. Ho halo atualizasaun simples duni. Kliente sira provavelmente atualiza no obten koresaun seguransa sempre liutan no lalais. Fabrikante software sira tenke orienta kliente sira agresivamente hamutuk ho atualiza trajetu ne'ebé redus risku kliente nian.

5. **Implementa alerta ne'ebé atrai atensaun.**
Hanesan ho sinu sintu seguransa iha karreta laran ne'ebé kontinua beibeik halo lian barullu kuandu la hatais sintu seguransa, fabrikante sira tenke implemente iha tempu los no repete alerta kuandu uzuariu ka administradór sira iha kondisaun la seguru duni, avizu administradór sira katak sira uza hela protokolu dezkontinuadu iha sira-nia ambiente no sujere atualiza trajetu sira. Implementa iha tempu los no repete alerta kuandu uzuariu ka administradór sira ka konfigurasaun aplikativu iha kondisaun la seguru. Halo modu la seguru ho klaru ba administradór sira iha baze regular. Rekursu adisional bele obriga superadministradór rekoñese fallta MFA iha sira-nia konta ba kada login, ka to'o dezativu determinadu rekursu prinsipal to'o sira ativa fali MFA. Iha espasu atu inova hodi atinji objetivu sira ne'e embora la kira alerta fadigu.

6. **Kria modelu konfigurasaun seguru.**
Modelu sira ne'e bele konfigurasaun determinadu atu seguru konfigurasaun baze ba apetite risku organizasaun ida. Embora maski simples duni iha modelu seguransa baixa/média/alta, ne'ebé ezemplu ilustra konfigurasaun hira bele atualiza atu jere risku ba organizasaun. Modelu sira bele suporta ho guia afrouximentu ba risku ne'ebé fabrikante identifika ona.

PRÁTIKA SEGURA DEZENVOLVIMENTU PRODUTU

1. **Dokumenta konformidade ba estrutura SDLC segura.** Estrutura SDLC segura fornese objetivu no ezemplu sira iha ema sira, prosesu no teknolojia hotu-hotu. Konsidera publika deskrisaun detalle ne'ebé segura kontrola estrutura SDLC implementa ona no deskreve kualkér kontroli alternativu ne'ebé uza ona. Iha US laran, konsidera uza Estrutura Dezenvolvimentu Software Seguru NIST (SSDF). Embora laos lista verifikasaun ida, SSDF "deskreve konfigurasaun prátika sólidu no fundamental hodi dezenvolve software seguru".

2. **Dokumenta Objetivu Dezempeñu Seguransa Sibernétika (CPG) ka konformidade ekivalente.** Kuandu organizasaun ida atestadu katak sira konforme ba padraun NIST SSDF, sira afirma katak sira-nia SDLC informa ona ho prátika melloria mak komprende ho di'ak. Entantu, la sufisiente ba sira hetan deit robusta SDLC ida. Sira mós tenke proteje sira-nia empreza rasik no dezenvolve ambiente husi ator malisiozu sira ne'ebé ba buka atu manipula propriedade seguransa produtu kuandu nia dezenvolve hela. Ida ne'e laos klasse teórika atake, maibe ida ne'ebé realiza ona ho efeitu adversu ba kliente sira, no ho estensaun seguransa nasional. Organizasaun tenke konsidera publika detalle kona-ba organizasaun-nia konformidade ba CISA CPG, Estrutura Sibernétika NIST (CSF), ka estrutura programa sibernétika seluk.

3. **Jerensiamentu vulnerabilidade.** Fabrikante balun iha programa jerensiamentu vulnerabilidade ida iha vulnerabilidade koresaun deskobre internamente ka esternamente no oituan tan. Programa madura liutan inkorpora analize estensa vulnerabildiade no sira-nia kauza prinsipal, foti etapa atu elimina sistematikamente klasse vulnerabilidade hotu-hotu[3]. Sira implementa programa formal iha konfigura planeamentu, kualidade, kontrolu, melloria kualidade no medisaun kualidade. Sira hare jerensiamentu nia defeitu nu'udar problema negosiu ida, laos problema seguransa baibain deit. Programa sira ne'e la hanesan iha medidas balu ba programa kualidade no seguransa iha industria seluk.

4. **Responsabilidade uza software kódigu abertu.** Kuandu software kódigu abertu uza ona, sai responsavel ho verifika pakote kódigu abertu, promove kontribuisaun kódigu retornu ba dependensia, no ajuda sustenta dezenvolvimentu no manutensaun komponentu kritikal sira. Ba referênsia, Ministériu Ekonomia, Komérsiu no Indústria (METI) Japaun publika ona "Kolesaun Ezemplu Kazu Uza Relativu Métodu Jerensiamentu atu Utiliza OSS no Garante Ninia Seguransa."

5. **Fornese padraun seguru ba dezenvolvedór sira.** Halo rota padraun durante dezenvolvimentu software ida ne'ebé seguru ho fornese bloku konstrusaun seguru ba dezenvolvedór sira. Por ezemplu, hanoin ba prevalênsia vulnerabilidade injesaun SQL kauza danus iha mundu real, garante katak dezenvolvedór sira uza biblioteka mantidu atu prevene klasse vulnerabilidade ne'eba. Ne'e mós koñesidu nu'udar "estrada pavimentadu" ka "kamiñu iluminadu", prátika sira ne'e garante sira rua ba velosidade no seguransa, no redus erru humanus.

6. **Promove forsa traballu dezenvolvedór software ne'ebé komprende seguransa.** Garante katak Ita-nia dezenvolvedór software nian komprende seguransa ho treinu sira kona-ba prátika rekomenda ba kodifikasaun segura. Aléinde, ajuda transforma forsa traballu jeral ho atualiza prátika kontratasaun atu avalia koñesimentu seguransa no traballu ho universidade sira, fakuldade komunitária, bootcamp sira no edukadór sira seluk atu integra seguransa tama ba siênsia komputasaun no dezenvolvimentu software.

[3] NIST SSDF, PO 1.2, Ezemplu 2: "Define polítika ne'ebé espesifika rekizitu seguransa ba software organizasaun nian no verifika konformidade iha pontu-xave SDLC (por ezemplu, klasse falla software verifikadu ho porta, resposta ba vulnerabilidade deskoberta iha software lansadu ona)."

7. **Teste jerensiamentu eventu insidente seguransa (SIEM) no integrasaun orkestrasaun, automasaun no resposta seguransa (SOAR).** Aléinde realiza teste kampu, traballu hamutuk ho provedór SIEM no SOAR popular sira konjuntu ho kliente selesionadu sira atu komprende oinsá ekipa responde insidente uza logs atu investiga suspeitu ka insidente seguransa atual. Dezenvolvedór software balun iha esperiênsia atu responde insidente ida no bele kria entrada log ne'ebé la ajuda respondente sira hanesan sa'ida sira espera ona. Traballu hamutuk ho teknolojia SIEM no SOAR no profisional real resposta insidente sira, ekipa dezenvolvimentu bele kria logs ne'ebé konta istória koreta no kompleta, ekonomiza tempu no redus inserteza durante insidente.

8. **Aliña ho Zero Trust Architecture (ZTA).** Aliña guia implantasaun produtu, por ezemplu, modelu NIST ZTA no modelu CISA Zero Trust Maturity. Enkoraja kliente sira atu inkorpora prinsipiu sira ne'e iha kliente sira-nia ambiente.

PRÁTIKA NEGÓSIU PRÓ-SEGURANSA

1. **Fornese rejistru kustu adisional.** Servisu Cloud tenke kompromete atu jera no armajen rejistru relasiona ho seguransa sein kustu adisional. Produtu lokal mós tenke jera logs relasiona ho seguransa sein kustu adisional. Aléinde, produtu tenke rejistru eventu seguransa tanba barak kliente la komprende sira-nia valór to'o insidente ida. Tátika sira ne'e karik presija revizaun kompleta kona-ba eventu seguransa sa'ida tenke rejistru atu fornese konsiênsia estadu seguransa sibernétika, oinsá kliente ida bele konfigura rejistru, to'o periodu tempu hira rejistru log, to'o bainhira integridade log no armajen proteje hela no oinsá log sira bele analiza. Iha kazu balun, revizaun bele sujere nesesidade ba refatorasaun husi arkuitetura jerensiamentu aplikativu rejistru nian atu ajuda halo sira asionável no iha kustu katak traballu ba fabrikante. Traballu ho profisional responde insidente (IR) bele aumenta oportunidade ne'ebé sei benefisiu ba investigadór sira iha kampu. Hare seksaun iha SIEMs.

2. **Elimina impostu subar hela.** Publika kompromisu atu nunka tau folin ba seguransa ka rekursu privadu ka integrasaun sira. Por ezemplu, iha eskopu boot liutan husi jerensiamentu identidade no asesu (IAM), iha servisu hanaran servisu logon úniku (SSO). Fabrikante balun sira tau folin liutan atu konekta sira-nia sistema ba servisu SSO ida (dalaruma refere nu'udar provedór identidade). "Impostu SSO" ida ne'e signifika katak jerensiamentu identidade no asesu di'ak ne'e mak labele alkanse ba SMOs barak, prevene sira husi alkanse postura seguransa forte. Servisu balun fó kustu liutan atu abilita MFA ba uzuáriu sira. **Seguransa labele tau folin nu'udar sasán luxu, mais konsidera nu'udar direitu kliente ida.** Fabrikante balun argumenta katak kliente hirak solisita rekursu sira ne'e, no sira kustu liutan atu mantein. Argumentu sira ne'e ignora faktu katak kliente hirak sei liga atu reklama ka negosia, loloos ne'e kliente balun la komprende benefisiu sa'ida husi rekursu sira ne'e, no katak rekursu hotu-hotu presija kustu manutensaun. Entantu, ami la hare barak fabrikante kobra estra ba disponibilidade ka integridade dadus. Kustu atu apoiu atributu-xave sira ne'e mak inklui iha presu mak kliente sira tenke selu, hanesan ho kustu mak inklui sintu seguransa, koluna dirsaun dobravel no airbags ne'ebé salva vida iha asidenti sira.

3. **Adota padraun abertu sira.** Implementa padraun abertu, espesialmente kona-ba rede komun no protokolu identidade sira. Evita protokolu proprietáriu kuandu padraun abertu disponivel.

4. **Fornese ekipamentu atualizasaun.** Barak kliente sira relutante atu adota versaun atualizadu nian husi produtu, inklui implanta rekursu foun no seguru liutan hanesan koneksaun rede seguru. Fabrikante software sira bele aumenta adosaun kliente husi atualizasaun foun sira ho fornese ekipamentu atu ajuda redus inserteza no risku. Oferese lisensa gratuitu ba kliente sira atu teste atualizasaun no koresaun iha ambiente teste ida nu'udar meius ida atu motiva kliente sira.

PRINSIPIU 2: Adota Transparênsia Radikal no Responsabilidade

ESPLIKASAUN

Fabrikante software sira tenke orgullu ba sira-nia aan iha fornese produtu seguru no protejidu, no mós diferensia sira-nia aan husi sira seluk iha komunidade fabrikante baze ba sira-nia kapasidade atu halo hanesan ne'e.

Mai ita rezolve preokupasaun komun kona-ba transparênsia Kuandu profisional sira deskute transparênsia radikal, iha tendênsia ba konversa ne'e para iha preokupasaun katak sira fornese hela "roteiru ba atakante sira". Entantu, evidênsia barak katak atakante sira halo di'ak sein roteiru hanesan ne'e, no preokupasaun hanesan ne'e tenke fika iha segundu planu relasiona ho transparênsia ne'ebé benefisia kliente diretu, kliente indiretu, kadeia suprimentu no s diretos, indústria software tomak.

Transparênsia ajuda indústria estabelese konvensaun – signifika seluk, sa'ida mak parese "di'ak". Nia ajuda konvensaun sira muda iha tempu ba tempu atu responde ba kliente-nia nesesidade ba mudansa iha tátika ka ekonomia ator sira, ka evolusaun teknolojia. Transparênsia ajuda fabrikante sira ho rekursu oiutan deit aprende husi sira ne'eba ho rekursu madura no kapasidade barak liutan. Konversa kona-ba kompartilla informasaun tenke haluan liuhusi indikadór ameasa tempu real, atu inklui elementu sira iha kraik.

Transparênsia forsa dezisaun kona-ba seguransa atu foti sedu liu iha prosesu dezenvolvimentu no sai atividade kontinua beibeik ba líder empresarial sira, no mós

enjeñeiru no profisional seguransa sira. Transparênsia konstrui responsabilidade iha produtu laran.

Nota kona-ba hili adjetivu "radikal" molok lia-fuan "transparênsia". Ohin loron, la komun ida ba fabrikante software sira atu publika informasaun detalle kona-ba oinsá sira dezenvolve no mantein software no oinsá sira amadura sira-nia programa uza dadus husi tempu ba tempu. Iha indústria software nian, fabrikante balun oferese vizita guia kona-ba oinsá sira dezeñu sira-nia software. Iha oportunidade hirak ba fabrikante software ba hare oinsá organizasaun pare estrutura sira-nia programa SDLC, no oinsá programa sira ne'eba mantein iha ambiente kliente nian kontrak invasor real. Industria koletivu sei benefisiu husi kompartilla informasaun liutan kona-ba topiku hanesan estratejiku atu media kustu defeitu seguransa no atu elimina klasse vulnerabilidade. Nu'udar rezultadu husi pratika komun sira ne'e, fabrikante software hotu-hotu tenke aprende kona-ba oinsá infrenta rasik sira-nia seguransa produtu. Karik, la tau impostu ba sasán luxu iha rekursu seguransa, seguransa no protesaun tanba ne'e sai sentru kustu duke sentru lukru, no empreza hetan benefisiu ho hakma'an karga liuhusi kolaborasaun no transparênsia.

Ami hakarak foku ba tatika sira ne'ebé sei aselera materialmente evolusaun husi industria software. Ami la iha poder ona atu halo melloriamentu oportunidade no inkremental. Karik ita hakarak revolve ho koletivamente ba ameasa ne'ebé reprezenta husi adversáriu matenek no adaptivu, ita tenke adota nivel transparênsia ne'ebé sei sente la konfortu ohin loron, maibe sei diriji industria ba oin. Ohin loron iha fabrikante sira ne'ebé inkorpora balun prinsipiu seguransa tanba dezeñu sira ne'e. Hanesa William Gibson hatete, "futuru prontu iha ne'e, só deit ninia distribuisaun la justu". **Transparênsia radikal sei ajuda distribui informasaun ida ne'eba no fó benefisiu defensor liutan duke ami-nia adversáriu.**

Transparênsia bele halo liutan duke ajuda organizasaun pare amadura sira-nia SDLC. Kliente no investor prospektivu sira bele aprende liutan kona-ba investimentu no kompensasaun mak fabrikante sira halo ona, no postura seguransa sira mak investimentu kria ona ba kliente sira. Fabrikante sira ne'ebé adota transparênsia radikal sei fó kliente sira informasaun atu ajuda sira foti dezisaun ba kompras laos deit kona-ba folin no rekursu, maibe mós kona-ba seguransa hotu.

Organizasaun mak servisu makaas ona atu seguru sira-nia kadeia suprimentu no sira-nia SDLC, empreza sira konstrui ona sira-nia kompromisu prosesu foin dadauk ne'e. Adota transparênsia radikal tenke lidera ba divulgasaun publiku kona-ba atake no mós melloriamentu empreza mak halo ona atu prevene no detekta atake sira iha futuru. Forma informasaun mak kompartilla ne'eba sei ajuda organizasaun seluk aprende sein tenke sofre ba destinu hanesan.

DEMONSTRA PRINSIPIU IDA NE'E

Atu demonstra prinsipiu ida ne'e, fabrikante software sira tenke foti etapa sira inklui tuir mai:

PRÁTIKA SEGURU TANBA PADRAUN

1. **Publika estatístika no tendênsia relevante seguransa agregadu.** Ezemplu tópiku sira inklui adosaun MFA ho kliente no administradór sira no uza protokolu legadu inseguru.
2. **Publika estatístika koresaun sira.** Detalle porsentu sa'ida kliente mak iha produtu versaun atualizadu nian, no sa'ida lta halo atu atualiza ho fasil liutan no konfiável liutan.
3. **Publika dadus kona-ba priviléjiu naun utilizadu.** Publika informasaun agregadu kona-ba permisaun iha lta-nia kliente baze no mós insentivu sira no mudansa seluk ba produtu lta halo atu redus atake superfísie kliente nian. Priviléjiu la uza sira ne'e provavelmente sai kandidatu di'ak ba alerta administradór, hanesan sinu sintu seguransa nian.

PRÁTIKA SEGURA DEZENVOLVIMENTU PRODUTU

1. **Estabelese kontrola seguransa internu sira.** Barak empreza hare ona benefisiu husi muda sira-nia dadus ba fornesedór cloud sira. Agora fornesedór cloud sira sai tarjetu ba invasór sira. Software hanesan fornesedór Service (Saas) tenke publika estatistika ba sira-nia kontrola internu. Por ezamplu, fornesedór SaaS tenke publika kona-ba sira-nia implantasaun internu ba MFA rezistente phishing, hanesan autentikasaun Fast Identity Online (FIDO). Idealmente, sira tenke bele dehan katak la iha membru funsinariu bele asesu dadus sensitivu kliente ka seluk sein autentikasaun liuhusi MFA rezistente phishing.

2. **Publika modelu ameasa nivel altu sira.** Produtu seguru tanba dezeñu komesa ho modelu ameasa eskrita ona ne'ebé deskreve sa'ida kriadór tenta atu proteje no husi sé. Modelu ameasa efikas sira hetan informasaun liuhusi medidas intrusaun akontese iha fuik nian, no tenke kobre empreza no ambiente dezenvolvimentu sira, no mós medidas fabrikante software sira intende ba hodi atu uza iha ambiente kliente nian.

3. **Publika autoatestadu SDLC seguru detalle.** Fabrikante sira tuir NIST SSDF, ka estrutura seluk mak hanesan, ativamente traballu ba siklu vida dezenvolvimente software ida ne'ebé madura. Publikasaun auto-atestadu ida ne'ebé kontrola fabrikante promulga no ba produtu ida ne'ebé, sei demonstra kompromisu atu kumpri ba prátika melloria sira no fornese konfiansa no nivel aumenta ba sira-nia kliente. Eskema sertifikasaun seluk inklui Metodolojia Israel Cyber Supply Chain, por ezemplu.

4. **Adota transparênsia vulnerabilidade sira.** Publika kompromete ida ne'ebé sei garante katak produtu vulnerabilidade identifikadu sei publika nu'udar entrada CVE ne'ebé koretu no kompletu. Buat ne'e espesialmente vigór ba areia enumerasaun frakeza komun ne'ebé identifika kauza prinsipal ba vulnerabilidade sira. Koretu no kompletu liutan baze dadus CVE publiku, industria bele liu tanba buka oinsá produtu sira sai seguru liutan, no klasse vulnerabilidade ida ne'ebé mak sai prevalente. Entantu, kuidadu ho tentasaun ba konta CVE nian nu'udar métrika negativa, tanba númeru hanesan ne'e mós sinal ida husi komunidade saudável análize no teste kódigu. Ho fabrikante sira implementa filosofia seguru tanba dezeñu, posivel duni katak iha primeiru, sira-nia konta CVE brutu sei aumenta tanba deskobre komprehensivu liutan no koresaun vulnerabilidade sira iha kódigu ezistente. Fabrikante sira tenki publika analize vulnerablidade pasadu nian, inklui kualkér padraun no medidas sira mak foti ona atu rezolve klasse vulnerabilidade hotu-hotu. Por ezemplu, karik porsentajen boot husi CVE empreza nian relasiona ba cross-site scripting (XSS), dokumentasaun análize kauza prinsipal, responde (hanesan mudansa ba estrutura modelu web ne'ebé prevene XSS) no rezultadu sei sinaliza ba kliente sira katak sira sei sai vítima ho klasse vulnerabilidade tanba mitigasaun komprende ona durante durante dékada.

5. **Publika Lista Material Software (SBOMs).** Fabrikante sira tenke iha komandu ba sira-nia kadeia suprimentu. Organizations should build and maintain SBOMs [2] for each product, request data from their suppliers, and make SBOMs available for downstream customers and users. Ida ne'e sei ajuda demonstra sira-nia dilijênsia ba komprensaun komponente mak sira uza iha kriasaun sira-nia produtu, sira-nia kapasidade atu responde ba risku identifika ona foin dadauk ne'e, no bele ajuda kliente sira atu komprende oinsa atu responde karik modulu ida iha kadeia suprimentu foin hetan vulnerabilidade foun.

Nu'udar referênsia, Ministériu Ekonomia, Komérsiu no Indústria Japaun (METI) publika ona "Guia Introdusaun Lista Material Software (SBOM) ba jerensiamentu software". Transparênsia tenke estende ba firmware iha dispositivu inkorporadu sira no dadus no modelu sir amak uza iha IA/aprendizadu makina (ML). Aléinde ajuda ba dezisaun kompras nian no kapabilidade operasional sira, SBOMs kaer papél importante iha infraestrutura atu detekta no responde ba atake malisiozu kadeia suprimentu.

6. **Publika polítika divulgasaun vulnerabilidade sira.** Publika polítika divulgasaun vulnerabilidade sira ne'ebé (1) autoriza teste kontra produtu hotu-hotu, oferese ho fabrikante no kondisaun ba teste sira ne'e, (2) fornese traballu seguru legal ba asaun mak halo konsistente ho polítika, no (3) permite divulgasaun públika ba vulnerabilidade sira depois prazu tempu define ona. Fabrikante sira tenke realiza analize kauza prinsipal atu ba buka vulnerabilidade sira no halo maksimu duni karik posivel, foti asaun atu elimina klasse vulnerabilidade sira hotu. Hare ba Modelu Polítika Divulgasaun Vulnerabilidades CISA atu obten lingua referênsia.

PRÁTIKA NEGÓSIU PRÓ-SEGURANSA

1. **Nomeia publikamente patrosinadór ezekutivu sênior seguru tanba dezeñu.** Iha organizasaun barak, seguransa (hanesan kualidade) delega ba ekipa teknika ne'ebé iha kapasidade limitadu atu halo mudansa estrutural ba hadi'ak drastikamente seguransa produtu. Nomeia publikamente ezekutivu negósiu nivel altu ba supreviziona programa seguransa tanba dezeñu sei transforma seguransa produtu ba preokupasaun komersial nivel altu.

2. **Publika roteiru seguru tanba dezeñu.** Fabrikante sira tenke dokumenta alterasaun sira halo ba sira-nia SDLC atu melloria seguransa kliente nian, inklui detalle kona-ba relatóriu teste kampu, asaun mak foti ona atu elimina klasse tomak, no iten sira seluk mak lista iha prinsípiu sira seluk. Hanesan iha kazu esforsu melloria kualidade, programa melloria seguransa iha faze distinta ba planeamentu, kontrolu no melloria. Ho espíritu atu hatudu duke konta deit, publikasaun roteiru no detalle iha faze sira ne'e sei konstrui konfiansa ne'ebé produtu sira seguru tanba dezeñu. Depois alkanse ona progresu signifikativu, fabrikante sira bele detalle sira iha relatóriu transparênsia. Halo hanesan ne'e laos deit demonstra kompromete ida ba prinsipiu seguru tanba dezeñu maibe bele inspira sira seluk atu adota programa hanesan ho hatudu evidensia ezistente ida.

3. **Publika roteiru seguransa memória.** Fabrikante sira bele foti etapa hirak atu elimina klasse ida boot liu husi vulnerabilidade ho migrasaun produtu ezistente no konstrui produtu foun uza linguajen seguru ba memória. Embora ida ne'e la posível ba kazu hotu-hotu, fabrikante sira bele konsidera dezenvolve wrappers aplikativu iha linguajen seguru ba memória, duke eskrita fali aplikativu hotu-hotu. Ida ne'e mós bele inklui oinsá fabrikante sira atualiza kontratasaun, treinamentu, revizaun kódigu no prosesu internu sira seluk, no mós maneira sira ajuda comunidade kódigu abertu atu halo hanesan ne'e.

4. **Publika rezultadu.** Kuandu atualiza sira-nia SDLC para bele inkorpora filosofia seguransa tanba dezeñu ida, organizasaun sei ba buka manaan lalais, manaan lalais ho rekursu intensivu liutan, no kontratempu balun mak inesperadu. Ho reprezenta sira-nia susesu no obstákulu interna, industria tomak bele aprende husi rezultadu ne'e.

PRINSÍPIU 3: Lidera husi Tutun

ESPLIKASAUN

Embora filosofia jeral hanaran "seguransa tanba dezeñu", insentivu ba seguransa kliente nian komesa molok faze dezeñu produtu. Sira inisiu ho objetivu negosiu, objetivu implísitu no esplísitu no rezultadu mak espera ona. Só deit kuandu lider senior sira halo seguransa nu'udar prioridade negosiu, kria insentivu interna, no adota kultura tomak atu halo seguransa rekizitu dezeñu ida, sira sei alkanse rezultadu melloria.

Embora koñesimentu tékniku ne'e importante ba seguransa produtu niain, laos problema ida ne'ebé bele rezolve deit ba ekipa téknika. Ne'e mak prioridade negosiu ne'ebé tenke inisiu husi tutun.

Ema sira balun hanoin hela karik fabrikante software ida kaer metin prinsipiu rua primeiru nian no produs artefatu signifikativu, prinsipu terseiru ne'e nesesáriu ka? Oinsá empreza ida estabelese ninia vizaun, misaun, valór no kultura sei afeita produtu, no elementu sira iha komponente todan iha parte tutun. Ami hare ida ne'e iha industria seluk ne'ebé halo ona melloria dramatiku iha seguransa no kualidade. Famozu espesialista iha kualidade J.M. Juran eskreve:

> ***Obtensaun lideransa ho kualidade di'ak tenkiser jestór superior sira asumi pesoalmente ba jerente kualidade. Iha empreza ne'ebé la alkanse lideransa ho kualidade, jerente superior orienta pesoalmente inisiativu. Ha'u la iha koñesimentu kona-ba kualkér eksepsaun sira. [3]***

Ami fiar katak seguransa ne'e mak subkategoria kualidade produtu. Kuandu seguransa no kualidade sai imperativu negosiu no laos funsaun téknika ne'ebé submete totál ba ekipa téknika, organizasaun sira sei bele responde ba nesesidade seguransa sira-nia kliente lalais liutan no efisientemente. Aléinde, investe rekursu nesesáriu atu garante katak seguransa software ne'e prioridade negosiu prinsipal desde inísiu sei redus kustu prazu naruk ba rezolve defeitu software nian– no, to'o ninia tempu, diminui risku seguransa nasional.

Ho dalan hanesan ne'ebé ekipa lideransa implementa ona responsabilidade programa sosial korporativa (RSE), iha mós konsiênsia kresente katak konsellu korporativa sira, inklui fabrikante software sira, tenke asumi papel liutan ba orientasaun programa seguransa sibernétika. Termu responsabilidade sibernétika korporativa (CCR) dalaruma uza atu deskreve ideia ida ne'e mak mosu.

DEMONSTRA PRINSIPIU IDA NE'E

Atu demonstra prinsipiu ida ne'e, fabrikante software sira tenke foti etapa sira inklui tuir mai ne'e:

1. **Inklui detalle programa seguru tanba dezeñu ida iha relatóriu finanseiru korporativu sira.** Karik fabrikante ne'e empreza publiku, aumenta seksaun ida iha kada relatóriu dedikadu ba esforsu seguru tanba dezeñu. Buat komun ida ba relatóriu finanseiru annual automóvel nian atu inklui seksaun sira ba seguransa kondutór no pasajeiru sira, inklui informasaun kona-ba komité kualidade no seguransa sentralizadu no distribuí. Detallamentu programa tanba dezeñu iha relatóriu finanseiru sei demonstra katak organizasaun ne'e liga seguransa kliente no rezultadu finanseiru korporativu no laos deit adota termua material ida tanba ida ne'e famozu hela.

2. **Fornese relatóriu regular ba Ita-nia konsellu administrasaun.** Relatóriu diretór seguransa informasaun (CISO) ba konsellu korporativu jeralmente inklu informasaun kona-ba programa seguransa atual no planeadu, ameasa, insidente seguransa suspeitu no konfirmadu, no atualizasaun sentralizadu sira seluk iha postura seguransa no saúde empreza. Aleinde, atu simu informasaun kona-ba postura seguransa empreza nian, konsellu tenke husu informasaun kona-ba seguransa produtu no ninia impaktu ba seguransa kliente nian. Konsellu labele depende deit ba CISO, mais prinsipalmente ba membru sira seluk iha administrasaun empreza atu redus risku kliente niano.

3. **Kapasita ezekutivu seguru tanba dezeñu.** Iha diferente signifikadu entre organizasaun ida ne'ebé ekipa téknika iha "kompromisu ezekutivu," no sira ida ne'ebé lideransa negosiu personalmente jere prosesu adiatamentu seguransa kliente uza prosesu negosiu padraun. Termu "kompromisu ezekutivu" implika katak ema ida tenke faan ideia kona-ba programa seguransa kliente nian no laos sai objetivu negosiu nivel tutun. Ezekutivu ida ne'e tenke kapasita atu influensia investimentu produtu atu alkanse rezultadu seguransa kliente sira nian.

4. **Kria insentivu internu signifikativu sira.** Kuandu kuidadu hodi la kria insentivu perversu, aliña sistema rekompensa atu melloria seguransa kliente no koresponde komportamentu sira seluk no rezultadu valiozu. Husi seguransa tanba ezekutivu dezeñu to'o jerensiamentu produtu, dezenvolvimentu software, suporta, venda, legal no organizasaun sira seluk, inklui seguransa kliente ba kontratasaun, promosaun, salariu, bônus, opsaun asaun sira no prosesu komun seluk iha jestaun negósiu. Por ezemplu, kuandu estabelese kriteriu ba promove dezenvolvedór software sira, inklui konsiderasaun atu hadi'ak seguransa produtu hamutuk ho kriteriu seluk hanesan tempu ativu, dezempeñu no melloria rekursu.

5. **Kria konsellu seguru tanba dezeñu.** Iha industria balun, komun ba organizasaun sira atu kria konsellu kualidade sentraliza no inkorpora reprezentante kualidade iha divizaun prinsipal ka unidade negosiu. Ho inklui membru sentralizadu no distribuídu, grupu sira ne'e traballu atu melloria kualidade kontra objetivu nível superior, mesmu simu telemetria husi profundeza organizasaun. Mesmu mós, seguransa tanba dezeñu konsellu nian sei melloria seguransa kontra objetivu dezeñu organizasaun tomak.

6. **Kria no evolui konsellu kliente.** Fabrikante software iha konsellu kliente barak ne'ebé kompostu husi rejiaun, industria no tamañu diferente. Konsellu sira ne'e bele fornese informasaun barak kona-ba susesu kliente nian no dezafiu atu implanta produtu empreza nian. Estruture ajenda konsellu ho tópiku dedikadu rezolve seguransa kliente, mesmu ida ne'e laos prioridade atualmente ba partisipante sira. Konsidera iha ne'ebé konsellu kliente reporta no oinsá para partisipante sira obten koñesimentu kona-ba seguransa produtu kuandu implanta. Por ezemplu, konsellu iha tendênsia ba objetivu merkadolojia no venda ka ba jestaun produtu? Ezekutivu seguru tanba dezeñu tenke ajuda diriji interasaun kliente sira no tenke liga ho elementu sira seluk iha dokumentu ida ne'e, hanesan estudu kampu.

SEGURANSA TANBA TÁTIKA DEZEÑU

Estrutura Dezenvolvomentu Software Seguru/Secure Software Development Framework (SSDF), ne'e mós koñesidu nu'udar National Institute of Standards and Technology (NIST) SP 800-218, ne'e mak prátika konjuntu baziku dezenvolvimentu software seguru nivel altu ne'ebé bele integra ba kada estáju siklu vida dezenvolvimentu software (SDLC). Prátika tuir mai sira bele ajuda produtór software sira sai efikas liutan atu ba buka no hasai vulnerabilidade sira iha software mak publika ona, mitiga impaktu potensial husi esplorasaun vulnerabilidade sira no rezlove kauza prinsipal husi vulnerabilidade atu prevene akontese fali iha futuru.

Organizasaun autora enkoraja uza tátika seguru tanba dezeñu sira, inklui prinsipiu ne'ebé refere prátika SSDF sira. Fabrikante software sira tenke dezenvolve roteiru eskritu ida atu adota prátika dezenvolvimentu software seguru tanba dezeñu liutan iha sira-nia portfólio tomak. Tuir mai ne'e mak lista ilustrativa naun exaustiva husi prátika roteiru melloria sira:

- **Linguajen programasaun segura memória (SSDF PW.6.1).** Prioritiza uza lingua seguru memória iha ne'ebé posivel. Organizasaun autora rekoñese katak mitigasaun espesifiku memória bele ajuda tátika prazu badak ba kódigu baze legadu sira. Ezemplu sira inklui melloria linguajen C/C++, mitigasaun hardware, randomizasaun layout espasu enderesu (ASLR), integridade fluksu kontrola (CFI) no difusaun. Entantu, iha konsensu mak aumenta book katak adosaun linguajen programasaun seguru memória bele elimina klasse defeitu ida ne'e, no fabrikante software sira tenke esplora medidas atu adota sira. Ezemplu balun husi linguajen seguru memória inklu C#, Rust, Ruby, Java, Go no Swift. Lee seguransa memória NSA nia folla informasaun atu hatene liutan.
- **Baze Hardware seguru.** Inkorpora rekursu arkuitetura ne'ebé permite protesaun memória refinadu, hanesan sira mak deskreve ona ho Instrusaun RISC Aprimora Hardware Kapasidadea (CHERI), ne'ebé bele estende Arkuitetura Konjuntu Instrusaun (ISAs) hardware konvensional, no mós rekursu seluk hanesan Plataforma Konfiável no Módulu Seguransa Hardware . Ba informasaun liutan vizita, Universidade Cambridge-nia pajina web CHERI.
- **Komponente Software Seguru(SSDF PW 4.1).** Hetan no manten komponente software proteje ho di'ak (p.e., biblioteka software, módulu, middleware, estrutura) husi desenvolvedór komersial, kódigu abertu no terseiru verifikadu atu garante seguransa robusta iha produtu software konsumidór nian.
- **Estrutura modelu Web (SSDF PW.5.1).** Uza estrutura modelu Web ne'ebé implementa escape automátiku husi entrada uzuáriu hodi evitar atake ba Web, hanesan script entre site sira.
- **Kestaun parametrizadu (SSDF PW 5.1).** Uza kestaun parametrizadu duke inklui entrada uzuáriu iha kestaun sira, atu evita atake injesaun SQL.
- **Teste seguransa aplikativu estátiku no dinâmiku (SAST/DAST)** (SSDF PW.7.2, PW.8.2). Uza ekipamentu sira ne'e atu analize kódigu rekursu produtu no komportamentu aplikativu atu detekta prátika propenza erru sira. Ekipamentu sira ne'e kobre problema sira desde jerensiamentu inadekuadu ba memória to'o konstrusaun konsulta banku dadu propenza erru sira (por ezemplu, entrada uzuáriu sein halai ne'ebé direita ba injesaun SQL). SAST no DAST bele inkorpora ba prosesu dezenvolvimentu no la'o automatikamente nu'udar parte husi dezenvolvimentu software nian. SAST no DAST tenke komplementa tipu teste sira seluk, hanesan teste unitáriu no teste integrasaun, atu garante produtu sira kumpri ho rekizitu seguransa mak espera ona. Kuandu problema identifika ona, fabrikante sira tenke realiza analize kauza prinsipal nian atu rezolve vulnerabilidade sistematikamente.

- **Revizaun kódigu** (SSDF PW.7.1, PW.7.2). Esforsa atu garante katak kódigu hatama ba produtu laran passa téknika kontrola kualidade hanesan revizaun kolega ho dezenvolvedór sira seluk ka "propragasaun erru".
- **Lista Material Software (SBOM)** (SSDF PS.3.2, PW.4.1). Inkorpora kriasaun SBOM[4] atu fornese visibilidade tam ba konfigurasaun software ne'ebé implanta ba produtu laran.
- **Programa Divulgasaun Vulnerabilidade** (SSDF RV.1.3). Estabelese programa divulgasaun vulnerabilidade ne'ebé permite peskizadór seguransa sira ba relata vulnerabilidade sira no simu traballu legamente seguru atu halo ne'e. Nu'udar parte husi ida ne'e, fornesedór tenke estabelese prosesu atu determina kauza prinsipal husi vulnerabilidade mak kobre ona. Prosesu hanesan ne'e tenke inklui determina karik adota kualkér prátika seguru tanba dezeñu sira iha dokumentu ida ne'e (ka prátika sira seluk) tenke prevene introdusaun vulnerabilidade ne'e.
- **Kompletu CVE.** Garante katak CVEs publikasaun tenke inklui kauza prinsipal ka enumerasaun pontu fraku komun sira (CWE) hodi permite análize falla dezeñu seguransa software iha industria tomak. Embora garante katak kada CVE koretu no kompletu bele han tempu estra, ne'e permite entidade diferente atu identifika tendênsia ne'ebé fó benefisiu ba fabrikante no kliente hotu-hotu. Atu obten informasaun liutan kona-ba jerensiamentu vulnerabilidade, haree ba Orientasaun Kategorizasaun Vulnerabilidade Espesífika Parte Interesadu (SSVC) da CISA.
- **Defeza iha Profundidade.** Dezeña infraestrutura para komprometimentu ba kontrola seguransa úniku la rezulta ho kompromisu ba sistema tomak. Por ezemplu, garante katak priviléjiu uzuáriu provisionadu ho restrita no lista kontrola asesu mak empregadu ona bele redus impaktu husi konta kompromete ida. Aléinde, téknika sandbox software bele koloka vulnerabilidade iha kuarentena hodi limita komprometimentu husi aplikativu tomak.
- **Satisfa tarjetu dezempeñu seguransa sibernétika (CPGs).** Dezeñu produtu ne'ebé hasoru prátika seguransa baziku sira. Objetivu Dezempeñu Segurança Sibernétika CISA nian deskreve medida báziku no fundamental ba seguransa sibernétika ne'ebé organizasaun tenke implementa. Aléinde, ba maneira barak liutan atu fortifika lta-nia organizasaun postura, haree ba Estrutura Avaliasaun Sibernétika Reinu Unidu, ne'ebé kompartilla similaridade ho CPGs nia CISA. Karik fabrikante ida falla ba kumpri CPGs — hanesan la eziji MFA rezistente ba phishing ba funsionáriu sira hotu — entaun sira labele konsidera nu'udar fornese produtu seguru tanba dezeñu.

Organizasaun autora rekoñese katak mudansa hirak ne'e hanesan mudansa signifikadu iha postura organizasaun nian. Tanba ne'e, sira-nia introdusaun tenke prioritiza baze ba modelajen ameasa personalizadu, kritisidade, kompleksidade no impaktu negosiu. Prátika sira ne'e bele introdus ba software foun no espande gradativamente atu kobre kazu uza sira no produtu adisional sira. Iha kazu balun, kritisidade no postura risku produtu determinadu bele impede kronograma aseleradu atu adota prátika hirak ne'e. Iha nasaun seluk, prátika sira bele introdus iha baze kódigu legadu no korijidu husi tempu ba tempu.

[4] Organizasaun balun esplora hela abordajen alternativu atu obten garantia seguransa kona-ba kadeia fornesementu software.

TÁTIKA SEGURA TANBA PADRAUN

Aléinde atu adota prátika dezenvolvimentu seguru tanba dezeñu, organizasaun autora rekomenda ba fabrikante sotware sira atu prioritiza konfigurasaun seguru tanba padraun iha sira-nia produtu. Sira ne'e tenke esforsu atu atualiza produtu hodi konforme ba prátika hirak ne'e tanba sira atualizadu ona. Por ezemplu:

- **Elimina seña padraun.** Produtu sira la bele mai ho seña padraun ne'ebé distribui universalmente. Atu elimina seña padraun, organizasaun autora sira rekomenda produtu sira presija administradór atu konfigura seña ida mak forte durante instalasaun no konfigurasaun ka ba produtu atu embarka ho seña forte no uniku ba kada dispositivu.

- **Obriga autentikasaun multifatór (MFA) ba uzuáriu privilejiadu sira.** Ami observa katak barak implantasaun emprezarial sira jere ho administradór ne'ebé la proteje sira-nia konta ho MFA. Konsidera katak administradór sira tarjetu ho valór aas, produtu sira tenke halo MFA opt-out duke opt-in. Aléinde, sistema tenke husu ba administradór regularmente atu rejistru iha MFA to'o sira susesu bele ativu iha sira-nia konta. NCSC Ólanda iha orientasaun ne'ebé hanesan ho CISA, visita sira Folla Informativa Sobre Autentikasaun Adultu hodi obten informasaun liutan.

- **Logon úniku (SSO).** Aplikativu TI tenke implementa suporta logon úniku liuhusi meiu padraun aberta modernu. Hanesan ezemplu sira inklui Security Assertion Markup Language (SAML) ka OpenID Connect (OIDC). Rekursu ida ne'e tenke disponibiliza hamutuk ho padraun, sein kustu adisional.

- **Rejistu/logon ho seguru.** Fornese rejistru auditoria ho kualidade alta ba kliente sira ho sei kustu adisional ka konfigurasaun adisional. Rejistru auditoria ne'e mak krusial atu detekta no eskala insidente seguransa mak posivel. Sira mós krusial durante investigasaun ba suspeitu ida ka insidente seguransa konfirmadu ona. Konsidera prátika melloria hanesan fornese integrasaun fásil ho sistema jerensiamentu eventu no informasaun seguransa ho asesu ba interface programasaun aplikativu (API) ne'ebé uza oráriu universal koordenadu (UTC), formatasaun fuso oráriu padraun no téknika robusta dokumentasaun.

- **Perfil Autorizasaun Software.** Fornesedór software sira tenke fornese rekomendasaun kona-ba funsaun perfil autorizadu no kazu ba uza mak dezignadu. Fabrikante sira tenke inklui avizu visível ne'ebé notifika kliente sira kona-ba risku aumenta ona karik sira desvia husi autorizasaun perfil mak rekomenda ona. Por ezemplu, médiku bele vizualiza rejistru pasiente hotu, maibe ajendador médiku ida iha aseso limitadu atu determina informasaun nesesáriu ba ajendamentu konsulta sira.

- **Seguransa voltadu ba futuru kompara ho kompatibilidade versaun anterior.** Dalaruma, rekursu legadu anterior kompatível inkluí hotu, no dalaruma ativadu, iha produtu sira, maski kauza risku ba seguransa produtu nian. Prioritiza seguransa duke kompatibilidade versaun anterior nian, empoder ekipa seguransa atu hasai rekursu la seguru maski karik ida ne'e signifika ba kauza alterasaun signifikativu.

- **Rastrea no redus tamañu "guia enduresimentu".** Redus tamañu husi "guia enduresimentu" ne'ebé inkluí ho produtu no esforsa atu garante katak tamañu diminui iha tempu tanba versaun foun software nian lansa ona. Integra komponente husi "guia

enduresimentu" nu'udar konfigurasaun padraun produtu nian. Organizasaun autora sira rekoñese katak guia enduresimentu badak rezulta husi parseria kontinua ho kliente ezistente sira no inklui esforsu ho ekipa produtu barak, inklui esperiênsia uzuáriu (UX).

- **Konsidera konsekuênsia esperiênsia uzuáriu husi konfigurasaun seguransa.** Kada konfigurasaun foun aumenta karga kognitiva ba uzuáriu final sira no tenke avalia iha konjuntu ho benefísio komersial mak nia hetan. Idealmente, konfigurasaun labele eziste; kontrariu, konfigurasaun seguransa prinsipal tenke integra tama ba produtu liuhusi padraun. Kuandu konfigurasaun necesáriu, opsaun padraun tenke seguru luan tan kontra ameasa komun sira.

Organizasaun autora sira rekoñese mudansa sira ne'e bele iha efeitu operasional kona-ba oinsá software ne'e implementa. Tantu, opiniaun kliente ne'e mak kritikal atu balansu konsiderasaun operasional no seguransa sira. Ami fiar katak dezenvolve roteiru eskrita nian no apoiu ezekutivu ne'ebé prioritiza ideia sira ne'e tama ba produtu importante kritikal organizasaun nian hanesan etapa primeiru atu muda ba prátika seguru dezenvolvimentu software. Embora opiniaun kliente sira ne'e importante, ami observa ona kazu importante sira ne'ebé kliente sira lakohi ka la bele adota padraun aprimoradu, dalaruma protokolu rede nian. Importante ba fabrikante sira ba kria insentivu signifikadu ba kliente sira atu mantein atual no la permite nafatin vulneravel indefinidamente.

GUIA ENDURESIMENTU VS AFROUXAMENTU

Guia enduresimentu bele rezulta husi menus ba kontrola seguransa produtu nian mak implanta ba arkuitetura produtu nian desde inisiu dezenvolvimentu. Konsekuentemente, guia enduresimentu mós bele sai roteiru ba inimigu atu dezide no esplora rekursu mak la seguru. Buat komun ida ba organizasaun barak la sai siente kona-ba guia enduresimentu sira, maski sira husik sira-nia konfigurasan dispositivu iha postura la seguru. Modelu inverte koñesidu nu'udar guia afrouxamentu tenke troka guia enduresimentu hanesan ne'e no esplika alterasaun ida ne'ebé uzuáriu sira tenke halo mesmu mós halo lista rezultadu risku seguransa nian. Guia sira ne'e tenke hakerek ho profisional seguransa sira mak bele esplika kompenzasaun iha lingua klaru atu aumenta oportunidade aplika sira ne'e koretamente.

Duke dezenvolve guias enduresimentu ne'ebé lista métodu sira atu proteje produtu, organizasaun autora rekomenda fabrikante software sira muda ba abordajen seguru tanba padraun no fornese "guia de afrouxamentu". Guia sira ida ne'e esplika risku komersial husi dezisaun ho lingua simples no bele aumenta konsientizasaun organizasional kona-ba risku invasaun sibernétika malisioza. Kompenzasaun seguransa tenke determina ho kliente-nia ezekutivu senior, ekuilibra seguransa ho rekizitu negósiu sira seluk.

REKOMENDASAUN HIRAK BA KLIENTE SIRA

Organizasaun autora rekomenda organizasaun sira mantein responsabiliza fabrikante software fornesedór ba rezultadu seguransa husi sira-nia produtu hirak. Nu'udar parte husi ida ne'e, organizasaun autora sira rekomenda katak ezekutivu sira prioritiza importânsia ba sosa produtu ho seguru tanba dezeñu no seguru tanba padraun. Ida ne'e bele manifesta liuhusi estabelesementu polítika ne'ebé obriga departementu TI asesu seguransa software molok ba sosa ida ne'e, no mós kapasita departementu TI ba rejeita karik nesesáriu. Departamentu TI tenke kapasita atu dezenvolve kritériu sira ne'ebé enfaze importânsia prátika seguru tanba dezeñu no seguru tanba padraun (tantu sira rua deskrita iha dokumentu ida ne'e no sira seluk dezenvolve husi organizasaun). Aleinde, departamentu TI tenke hetan apoiu husi jestaun ezekutiva kuandu aplika kritériu sira tama ba dezisaun kompra sira. Dezisaun organizasional atu aseita risku mak asosiadu ho produtu teknolójiku espesífiku sira tenke dokumentadu formalmente, aprovadu ho ezekutivu emprezarial sénior no aprezenta regularmente ba konsellu administrasaun.

Prinsipal servisu TI emprezarial ne'ebé suporta postura seguransa organizasaun, hanesan rede emprezarial, jestaun identidade no asesu emprezarial no operasaun seguransa no kapasidades resposta, tenke haree nu'udar funsaun negósiu krítika ne'ebé finansiadu atu alinha importânsia sira nian ba susesu misaun organizasaun. Organizasaun tenke dezenvolve planu ida atu atualiza kapasidades sira ne'e hodi alavansa fabrikante sira ne'ebé adota prátika seguru tanba dezeñu no seguru tanba padraun.

Iha ne'ebé posível, organizasaun tenke esforsa ba estabelese relasaun estratéjika ho sira-nia fornesedór TI prinsipál. Relasaun ne'e inklui konfiansa iha váriu nível organizasaun no fornese veíkulu hirak atu rezolve problema no identifika prioridade partilladu sira. Seguransa tenke sai elementu krítiku ida husi relasaun hanesan ne'e no organizasaun tenke esforsa ba reforsa importânsia prátika segura dezeñu no seguru tanba padraun sira rua tama ba dimensaun formal (por ezemplu, kontratu ka akordu fornesedór sira) no informal husi relasaun ne'e. Organizasaun tenke espera transparênsia husi sira-nia fornesedór teknolojia sira kona-ba sira-nia postura kontrolu internu, no mós sira-nia roteiru ba adosaun prátika seguru tanba dezñu o seguru tanba padraun.

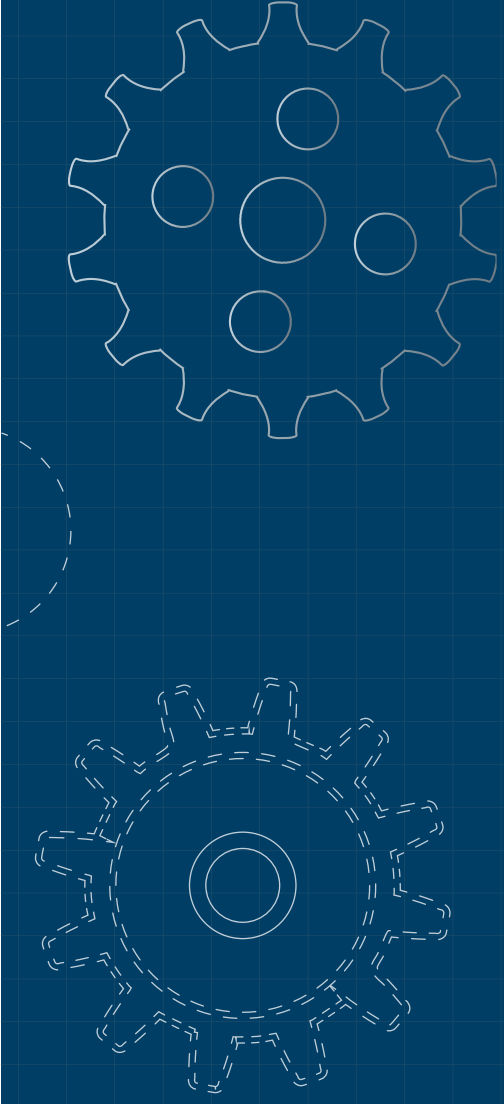
Aléinde atu halo seguransa tanba padraun iha organizasaun ida, líder TI sira tenke kolabora ho sira-nia parseiru setór industria atu komprende produtu no servisu ida ne'ebé mellor atu inkorpora prinsípiu dezeñu sira ne'e. Líder sira ne'e tenke koordena sira-nia pedidu atu ajuda fabrikante sira ba prioritiza sira-nia inisiativa seguransa ba futuru. Ho traballu hamutuk, kliente sira bele ajuda fornese informasaun signifikativu ba fabrikante sira no kria insentivu ba sira atu prioritiza seguransa.

Kuandu uza sistema cloud, organizasaun tenke garante sira komprende modelu responsabilidade ne'eé partilla ona ho sira-nia fornesedór teknolojia. Katak, organizasaun tenke iha klareza kona-ba responsabilidade seguransa fornesedór nian duke responsabilide kliente deit.

Organizasaun sira tenke prioritiza fornesedór cloud sira ne'ebé transparante kona-ba sira-nia postura seguransa, kontrola interna sira no kapasidade atu realiza sira-nia obrigasaun bazeia ba modelu responsabilidade mak distribui ona.

DESAPROVADÓR

Informasaun iha relatóriu ida ne'e fornese hela "loloos" ba objetivu informasional deit. CISA no organizasaun sira seluk la endosa kualkér produtu ka servisu komersial, inklui kualkér asuntu análize sira. Kualkér referênsia ba entidade komersial espesífika ka produtu sira, prosesu sira ka servisu komersial ho marka servisu, marka rejistradu, fabrikante ka forma seluk ne'ebé la konstitui ka implika endosu, rekomendasaun ka favoritismu parte CISA no organizasaun sira seluk. Dokumentu ida ne'e inisiativu konjuntu ho CISA ne'ebé automatikamente la servi nu'udar dokumentu regulatóriu.



Rekursu sira

CISA

- Orientasaun SBOM CISA nian
- Meta Dezempeñu Seguransa Sibernétika Intersetorial CISA
- Diretriz Sobre Interoperabilidade Teknolójika
- CISA no NIST's Defende Kontra Atake ba Software Kadeia Suprimentu
- Impaktu husi Teknolojia La Seguru no Sa'ida Ita Bele Halo Kona-ba Ida ne'e | CISA
- Para Passa Buck iha Seguransa Sibernétika: Tanba sa Empreza tenke Inklui Seguransa iha Produtu Teknolójiku sira (foreignaffairs.com)
- Orientasaun Kategorizasaun Vulnerabilidade Espesífika Parte Interesadu sira (SSVC) CISA
- Folla Téknika MFA Resistente Phishing CISA
- Orientasaun Sibernétika ba Empreza Kiik sira | CISA

NSA

- Folla Informasaun Seguransa Sibernétika NSA Sobre Seguransa Memória
- ESF NSA Proteje Kadeia Fornesimentu Software: Melloria Prátika ba Fornesedór sira

FBI

- Komprensaun no Responde ba Atake Kadeia Suprimentu SolarWinds: Perspektiva Federal
- Ameasa Sibernétika – Resposta no Relatóriu
- Estratéjia Sibernétika FBI

Institutu Nasional Padraun no Teknolojia (NIST)

- Diretriz Identidade Dijital NIST
- Estrutura Seguransa Sibernétika NIST
- Estrutura Dezenvolvimentu Software Seguru (SSDF) NIST

Sentru Australianu Seguransa Sibernétika (ACSC)

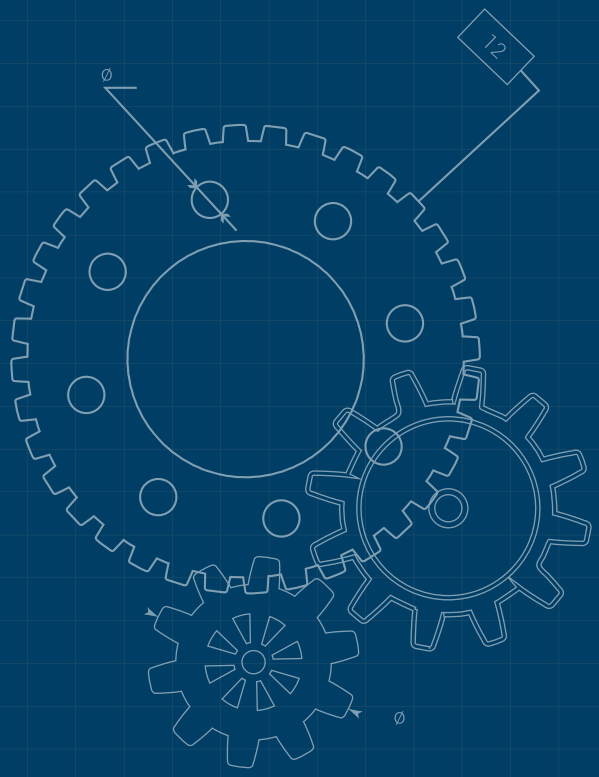
- Orientasaun Kódigu Prátika IoT ACSC ba Fabrikante sira

Sentru Nasional Seguransa Sibernétika Reinu Unidu (UK)

- Estrutura Avaliasaun Sibernétika Reinu Unidu
- Orientasaun Dezenvolvimentu no Implantasaun Seguru NCSC Reinu Unidu
- Orientasaun Jerensiamentu Vulnerabilidade NCSC Reinu Unidu
- Feramenta Divulgasaun Vulnerabilidade NCSC Reinu Unidu
- CHERI Universidade Cambridge
- Mak ne'e deit no obrigadu ba atensaun hotu-hotu - NCSC.GOV.UK

Sentru Kanadense Seguransa Sibernétika (CCCS)

- Orientasaun CCCS sobre Protesaun Kontra Atake hirak ba Kadeia Suprimentu Software nian
- Kadeia suprimentu sibernétika: Abordajen ida atu avalia risku sira
- Orientasaun Sobre ransomware CONTI Sentru Kanadense Seguransa Sibernétika



Eskritóriu Federal Seguransa Informasaun Alemanha (BSI)

- Kompêndiu BSI Grundschutz (módulu CON.8)
- Norma Internasional IEC 62443, parte 4-1
- Relatóriu Sobre Estado Seguransa TI iha Alemanha, 2022
- Prátika BSI Seguransa Aplikativu Web

Sentru Nasional Segurança Sibernétikaa Ólanda

- Folla informativa Sobre Autentikasaun Madura NCSC-NL nian

Sentru Nasional Preparasaun ba Insidente no Estratéjia ba Seguransa Sibernétika (NISC) Japaun

- Estratéjia Nasional Seguransa Sibernétika Japaun nian

Ministériu Ekonomia, Komérsiu no Indústria Japaun (METI)

- Guia Introdusaun Material Bill Software (SBOM) ba jerensiamentu Software
- Koleta Ezemplu sira ba Kazu Uza nian Relasiona ho Métodu Jerensiamentu baUtiliza OSS no Garante ninia Seguransa

Ajênsia Seguransa Sibernétika Singapura

- Akonsellamentu Tékniku sobre Dezenvolvimentu API Seguru
- Polítika Divulgasaun Vulnerabilidade CSA SingCERT
- Lista verifikasaun Resposta ba Insidente CSA SingCERT
- Manual Resposta ba Insidente CSA SingCERT
- Estrutura Seguransa CSA Bazeia Dezeñu
- Lista verifikasaun Estrutura Seguransa bazeia Dezeñu CSA
- Guia CSA ba modelajen Ameasa Sibernétika
- Eskema Rotulajen Seguransa sibernétika CSA

Seluk

- Nusá Sistema Kompleksu falla
- Vizual Foun falla iha sistema kompleksu

REFERÊNSIA

[1] https://csrc.nist.rip/publications/history/ande72.pdf

[2] https://www.cisa.gov/sbom and SBOMs references in TR 03183-2 https://www.bsi.bund.de/dok/TR-03183

[3] Juran on Quality by Design by J.M. Juran, 1992.