TLP:CLEAR

Muda Ekuilibriu Risku Seguransa Sibernétika: Prinsípiu no Abordajen sira ba Seguransa-ho-Dezeñu no -Padraun

Publikasaun: 13 Abril, 2023

Ajênsia Seguransa Sibernétika no Infraestrutura

NSA | FBI | ACSC | NCSC-UK | CCCS | BSI | NCSC-NL | CERT NZ | NCSC-NZ

Desaprovadór: Dokumentu ida ne'e marka ona TLP:CLEAR. Divulgasaun la limitadu. Fonte sira bele uza TLP:CLEAR kuandu informasaun aprezenta risku minimu ka la iha risku previsível ba uza inkoretu, akordu ho regras no prosidementu aplikável sira ba divulgasaun pública. Sujeitu ba regras direitu autoral padraun nian, informasaun TLP:CLEAR bele distribuí sein restrisaun. Ba informasaun liutan kona-ba Traffic Light Protocol, haree ba http://www.cisa.gov/tlp/.

Índise

VIZAUN JERAL: VULNERÁVEL HO DEZEÑU

Teknolojia ne'e integradu ba kuaze tomak kada faseta vida nian. Sistema konektadu Internet ne'e konekta hotu ba sistema krítiku ne'ebé impaktu diretamente ba ami-nia prosperidade ekonômika, meius subsistênsia nian no to'o saúde, husi jerensiamentu identidade pesoal to'o kuidadu médiku nian. Nu'udar ezemplu ida deit, violasaun sibernétika rezulta ona ho kanseladu sirurjia iha ospital laran hirak no muda atendementu pasiente ho globalmente. Teknolojia la seguru no vulnerabilidade iha sistema krítiku nia laran bele konvida invasaun sibernétika malisiozu, ne'ebé direta ba risku seguransa[1] potensialmente.

Agora, importante duni ba fabrikante teknolojia atu halo Seguru-ho-Dezeñu no Seguru-ho-Padraun nu'udar pontu fokal husi dezeñu produtu no prosesu dezenvolvimentu. Fornesedór balun halo ona progresu boot ba avansu setór industria iha garantia software, enkuantu sira seluk la dezenvolve. Ajênsia autorasaun sira enkoraja makaas ba kada fabrikante teknolojia atu halo sira-nia produtu iha meius ne'ebé prevene kilente sira husi obrigasaun ba monitora opera, atualiza rotina konstantemente no kontrola defeitu iha sira-nia sistema atu mitiga invasaun sibernétika nian. Fabrikante sira enkoraja ona atu asumi responsabilidade ba hadi'ak rezultadu seguransa husi sira-nia kliente. Istorikamente, fabrikante teknolojia sira depende ona ba hadi'ak vulnerabilidade mak hetan ona depois de kliente sira implanta produtu hirak, presija kliente sira ba taka falta/patches sira ho sira nia osan rasik. Só deit ho inkorpora pratika Seguru-ho-Dezeñu sira, ita sei bronkas sikulu aat husi kriasaun no aplika koresaun

Atu atinji padraun aas ida ne'e husi seguransa sibernétika, ajênsia autorasaun enkoraja fabrikante sira ba prioritiza integrasaun seguransa produtu nu'udar pré-rekuisitu krítiku ba rekursu no velosidade iha merkadu. Hamutuk ho tempu, ekipa enjiñeriu sira sei bele estabelese ritmu estável foun, ida ne'ebé seguransa dezeñu tebes no han tempu oituan atu mantein.
Reflete ba perspektiva ida ne'e, Uniaun Europeia reforsa kona-ba importansia husi seguransa produtu iha Cyber-Resilience-Act mak enfaze fabrikante sira tenke implementa seguransa tomak ba sikulu moris produtu nian hodi prevene fabrikante sira introdus produtu vulnerável sira tama ba merkadu laran.

Atu kria futuru ida ne'ebé teknolojia no produtu asosiadu sira sai seguru liutan ba kliente sira, ajênsia autorasaun insita fabrikante sira atu renova sira-nia dezeñu no dezenvolve programa ba permite deit produtu Seguru-ho-Dezeñu no -Padraun haruka ba kliente sira. Produtu sira mak Seguru-ho-Dezeñu ne'e mak sira ne'ebé seguransa kliente nian nu'udar objetivu negosiu prinsipál

[1] Ajênsia autorasaun rekoñese katak termu "seguransa" iha signifikasaun oinoin depende ba kontekstu utiliza nian. Ba objetivu husi guia ida ne'e, "seguransa" sei refere ba hasae padraun seguransa teknolojia sira atu proteje kliente sira kontra atividade sibernétika malisiozu.

nian, laos deit ba rekursu tékniku. Produtu Seguru-ho-Dezeñu nian komesa husi objetivu ida ne'eba molok inísiu dezenvolvementu. Produtu Seguru-ho-Padraun nian ne'e mak sira ne'ebé seguru atu kria "ideia kreativu" ho oituan ka la iha mudansa nesesariu ba konfigurasaun no rekursu seguransa disponivel sein kusta adisional. Hamutuk, prinsípiu rua sira ne'e transfere todan barak husi seguru nafatin ba fabrikante sira no redus oportunidade katak kliente sira sei sai vitima ba insidente seguransa tanba konfigurasaun sala, taka falta la sufiente, ka problema komum seluk barak liutan.

Ajênsia Seguransa Sibernétika no Infraestrutura (CISA), Ajênsia Seguransa Nasional (NSA), Departamentu Federal Investigasaun (FBI) no parseiru internasional sira hanesan tuir mai[2] fó rekomendasaun hirak iha guia ida ne'e ba fabrikante teknolojia sira atu garantia seguransa ba sira-nia produtu:

- Sentru Seguransa Sibernétika Australianu (ACSC)
- Sentru Kanadense Seguransa Sibernétika (CCCS)
- Sentru Nasional Seguransa Sibernétika Reinu Unidu (NCSC-UK)
- Eskritóriu Federal Seguransa Informasaun Alemaña (BSI)
- Sentru Nasional Seguransa Sibernétika Holanda (NCSC-NL)
- Ekipa Resposta Emerjênsia Informátika Nova Zelândia(CERT NZ) no Sentru Nasional Seguransa Sibernétika Nova Zelândia (NCSC-NZ).

Ajênsia autorasaun rekoñese kontribuisaun sira husi parseiru setór privadu barak ba avansu seguru-ho-Dezeñu no seguru-ho-Padraun. Produtu ida ne'e destina atu promove konversa internasional kona-ba prioridade prinsipál sira, investimentu no nesesariu dezisaun atu alkanse futuru ida ne'ebé teknolojia seguru, proteje no rezilente ho dezeñu no padraun. To'o parte ikus nian, ajênsia autorasaun ba buka opiniaun kona-ba produtu ida ne'e husi parte sira mak interese ona no hakarak konvoka série sesaun sira atu rona liutan ba refina, espesifika no avansu ami-nia guia atu alkanse ami nia objetivu kompartilla nian.

Ba informasaun liutan kona-ba importansia husi produtu mak seguru, haree ba artigu CISA nian, The Cost of Unsafe Technology and What We Can Do About It.

Seguru-ho-Dezeñu

"Seguru-ho-Dezeñu" signifika ba produtu teknolojia mak halo ona iha meius ida ne'ebé proteje razoalmente kontra atór malisiozu sira atu obten asesu ba dispositivu, dadus no konekta infraestrutura ho susesu. Fabrikante software sira tenke realiza avaliasaun risku atu identifika no enumera ameasa sibernétika predominante sira ba sistema kritiku, no depois

[2] Husi ne'e refere nu'udar "ajênsia autorasaun."

inklui protesaun iha projetu produtu nian ne'ebé konsidera senáriu ameasa sibernétika mak nafatin halo evolusaun.

Dezenvolvimentu pratika informasaun teknolojia (TI) mak seguru no vária xamada defesa—koñesidu nu'udar defesa iha profundade—ne'e mós rekomenda atu evita atividade inimigu ameasa sistema ka obten asesu naun autorizadu ba dadus sensitivu. Ajênsia autorasaun rekomenda fabrikante sira ba uza modelu ameasa mak personaliza ona durante estájiu dezenvolvimentu produtu ne'e atu rezolve ameasa potensial hotu-hotu ba sistema no konstabiliza ba kada prosesu implantasaun sistema nian.

Ajênsia autorasaun insita fabrikante sira simu abordajen seguransa holístika ba sira-nia produtu no plataforma sira. Dezenvolvimentu Seguru-ho-Dezeñu presija investimentu rekursu signifikadu husi fabrikante software sira iha kada xamada husi dezeñu produtu no proses dezenvolvimentu ne'ebé labele "aparafusadu" depois de. Presija lideransa forte husi ezekutivu aas fabrikante nian atu halo prioridade negosiu seguransa nian, laos deit iha rekursu tekniku nian. Kolaborasaun ida ne'e entre lider negosiu sira no ekipa tekniku sira, habelar husi estájiu inisiu ba dezeñu no dezenvolvimentu, liuhosi implantasaun kliente no manutensaun. Fabrikante sira hetan enkoraja atu halo konsesaun no investimentu sira, inklui ba sira mak sei sai "invisível" ba kliente sira, hanesan migrasaun ba programa lingua ne'ebé elimina vulnerabilidade boot liutan. Sira tenke prioritiza rekursu, mekanizmu no implementasaun ekipamentu sira ne'ebé proteje kliente sira husi rekursu produtu mak parese atrai maibe haluan superfisie atake nian.

La iha solusaun ida atu hakotu ameasa persistente husi ajente sibernétiku malisiozu atu esplora vulnerabilidade teknolojia, no produtu sira mak "Seguru-ho-Dezeñu" sei kontinua sofre vulnerabilidade sira; entantu, vulnerabilidade maioria tanba pekuenu relativemente kiik. Fabrikante sire tenke dezenvolve roteiru eskrita nian atu aliña sira nia portfólio produtu ezistente ho pratika Seguru-ho-Dezeñu liutan, garantia iha devia deit iha situasaun eksepsional nian.

Ajênsia autorasaun rekoñese katak asumi propriedade husi rezultadu seguransa ba kliente sira no garantia iha nivel seguransa kliente ida ne'e sei aumenta kusta dezenvolvimentu nian. Entantu, investimentu in pratika "Seguru-ho-Dezeñu" embora dezenvolve produtu teknolojia foun no mantein sira mak eziste ona, substansialmente hadi'ak postura seguransa kliente sira no redus probabilidade kompromitidu. Prinsipiu Seguru-ho-Dezeñu laos deit atu fortifika postura seguransa nian ba kliente sira no reputasaun marka ba dezenvolvedór sira maibe mós redus kusta manutensaun no taka falta iha periodu naruk nian.

Rekomendasaun ba fabrikante software sira nia seksaun lista ona iha kraik no fornese lista pratika no polítika dezenvolvimentu produtu ba fabrikante sira atu konsidera.

Seguru-ho-Padraun

“Seguru-ho-Padraun” signifika ba produtu ne'e reziliente kontra esplorasaun tekniku kreativu sein kusta adisional. Produtu hirak ne'e proteje kontra ameasa no vulnerabilidade prevalente sira sein uzuáriu final sira tenke foti medidas adisional atu proteje sira. Seguru-ho-Padraun ne'e dezeñu ona atu halo kliente sira konsiente duni katak bainhira sira devia husi padraun, sira aumenta probabilidade komprometidu nian só deit sira implementa kontrola kompensasaun adisional.

- Konfigurasanun mak proteje tenke sai liña baze padraun nian. Produtu Seguru-ho-Padraun sira abilita automatikamente kontrola seguransa mak presija atu proteje empreza sira husi atór sibernétiku malisiozu sira, no mós fornese kapasidade atu uza no konfigura liutan kontrola seguransa no la iha kusta adisional.
- Kompleksidade husi konfigurasaun seguransa laos atu sai problema ba kliente sira. Ekipa TI organizasaun sempre nakonu ho responsabilidade seguransa no operasional nian, nune'e rezulta ba tempu limitadu atu komprende no implementa implikasaun no mitigasaun seguransa mak presija ba postura robusta seguransa sibernétika. Liuhosi otimazasaun konfigurasaun produtu mak protejedu—proteje “pasajen padraun”—fabrikante sira bele ajuda sira-nia kliente ho garantia sira-nia produtu fabrikadu, distribui no uza ho seguransa akordu ho padraun "Seguru-ho-Padraun" nian.

Fabrikante produtu ne'ebé "Seguru-ho-Padraun" sira la tau kusta estra ba implementa konfigurasaun seguransa adisional nian. Kontrariu, sira inkorpora tama ba produtu baze hanesan sintu seguransa nian mak inklui iha kareta foun nia laran hotu-hotu. Seguransa laos opsaun luxu ida maibe besik liutan ba padraun mak kada kliente tenke espera sein negosia ka aumenta selu.

REKOMENDASAUN BA FABRIKANTE SOFTWARE SIRA

Guia konjuntu ida ne'e fornese rekomendasaun sira ba fabrikante sira atu dezenvolve roteiru eskritu atu implementa no garantia seguransa TI nian. Ajênsia autorasaun rekomenda ba fabrikante software sira ba implementa estratejia mak esplika ona iha seksaun kraik ne'e atu asumi propriedade rezultadu seguransa husi husi sira-nia kliente sira liuhosi prinsipiu Seguru-ho-Dezeñu no Padraun nian.

Prinsípiu Seguransa Produtu Software

Enkoraja ona ba fabrikante teknolojia sira atu adota foku estratejia mak prioritiza seguransa software nian. Ajênsia autorasaun dezenvolve ona prinsipu prinsipal tolu iha kraik atu guia fabrikante software sira ba halo seguransa software nian inkorpora ba sira-nia prosesu dezeñu nian molok atu dezenvolve, konfigura no haruka sira-nia produtu.

1. Problema seguransa loloos ne'e labele sai todan ba kliente. Fabrikante software sira tenke

asumi propriedade ba rezultadu seguransa husi kliente sosa ona no dezenvolve sira-nia produtu akordu ne'e.

2. Hakuak transparênsia no akuntabilidade radikal. Fabrikante software sira tenke orgullu sira-nia aan ba haruka produtu protejidu no seguru, no mós diferensia sira-nia aan entre fabrikante komunidade seluk baze ba sira nia kapasidade atu halo nune'e. Ida ne'e bele inklui fahe informasaun sira aprende husi implantasaun sira-nia kliente, hanesan uza mekanizmu autentikasaun forte ho padraun. Ne'e mós inklui kompromisu forte atu garante alerta vulnerabilidade no rejistru asosiadu vulnerabilidade no espozisaun komum (CVE) mak kompletu no ezatu. Entantu, kuidadu ho tentasaun atu konta CVE nu'udar métrika negativu, tanba númeru sira hanesan ne'e mós siñal análize kódigu saudável no komunidade teste.
3. Harii estrutura organizasional no lideransa atu alkanse objetivu hirak ne'e. Embora, esperiênsia téknika ba asuntu ne'e hanesan krítika ba seguransa produtu nian, ezekutivu senior hanesan tomador dezisaun prinsipál atu implementa mudansa iha organizasaun ida. Kompromisu nivel ezekutivu ba fabrika software sira atu prioritiza seguransa nu'udar elementu kritiku husi dezenvolvimentu produtu, presija parsieru hirak ho kliente organizasaun nian komprende ba:
    a. Orientasaun senáriu implantasaun hamutuk ho modellu ameasa personalizadu nian
    b. Implementasaun proposta ona ba kontrola seguransa aliña ho prinsipiu Seguru-ho-Padraun nian
    c. Estratejia alokasaun rekursu mak personalizadu ba empreza nia boot no kapasidade atu troka pratika dezenvolvimentu legadu ho pratika Seguru-ho-Dezeñu nian
    d. Nesesidade atu mantein liña komunikasaun nakloke ba opiniaun interna no esterna (p.e., opiniaun husi empregadu no kliente) kona-ba seguransa produtu nian. Seguransa software nian tenke enfaze iha forum internal (p.e., ho liman hotu-hotu kan bolsu maron), no mós marketing esterna no engajamentu kliente nian
    e. Medisaun efikásia iha implantasaun kliente nian. Lidera ezekutivu senior sei hakarak hatene kona-ba investimentu iha seguransa ho dezeñu no padraun atu ajuda kliente sira ho halo neineik pasu husi falta seguransa nian, redus erru konfigurasaun sira no minimiza superfisie atake.

Atu abilita prinsipiu tolu sira ne'e, fabrikante sira tenke konsidera tátiku operasional balun atu evolui sira-nia prosesu dezenvolvimentu.

Konvoka reuniaun rotina ho lideransa ezekutivu empreza nian atu diriji importansia husi Seguru-ho-Dezeñu no Seguru-ho-Padraun iha organizasaun nia laran. Politika no prosidementu tenke estabelese atu rekompensa ekipa produsaun ne'ebé dezenvolve produtu sira baze ba

prinsipiu sira ne'e, ne'ebé bele inklui rekompensa ba implementa pratika seguransa software estraordinariu ka insentivu ba eskala traballu no kritériu promosaun nian.

Opera ba importansia husi seguransa software ba susesu negosiu nian. Por ezemplu, konsidera atribui "lidre seguransa software nian" ka "ekipa seguransa software nian" ne'ebé kaer metin pratika negosiu no TI ba diretamente liga padraun seguransa no responsabilidade fabrikante nian. Fabrikante sira tenke garante sira iha robusta, avaliasaun independente seguransa produtu no programa evaluasaun ba sira-nia produtu.

Uza modellu ameasa personalizadu durante dezenvolvimentu atu prioritiza impaktu ba produtu mak kritiku liu no aas nian. Modellu ameasa sira konsidera produtu nia espifiku ba kazu uza nian no abilita ekipa dezenvolvimentu atu fortifika produtu sira. Afinal, lideransa sênior tenke kaer responsabilidade ekipa nian atu haruka produtu mak protejidu nu'udar elementu prinsipál husi produtu mak kapaas no kualidade.

Tática Seguru-ho-Dezeñu sira

Estrutura Dezenvolvimentu Software Protejidu (SSDF), mós koñese nu'udar Institutu Nasional ba Padraun no Teknolojia (NIST) SP 800-218, ne'e mak konjuntu baziku ba pratika seguru dezenvolvimentu software nian, ne'ebé bele integra ba kada estájiu husi sikulu moris dezenvolvimentu software nian (SDLC). Haktuir prátika hirak ne'e bele ajuda produtór software sira sai efikas liutan iha ba buka no hasai vulnerabilidade iha software mak lansa ona, mitiga impaktu potensial husi esplorasaun vulnerabilidade nian, no rezolve kauza prinsipal husi vulnerabilidade atu prevene mosu fali iha futuru.

Ajênsia autorasaun enkoraja utiliza tática Seguru-ho-Dezeñu nian, inklui prinsipiu sira mak refere ba pratika SSDF sira. Fabrikante software sira tenke dezenvolve roteiru eskritu atu adota pratika dezenvolvimentu seguru-ho-dezeñu nia iha sira-nia portofolio hotu-hotu. Tuir mai ne'e lista naun eksaustiva husi pratika roteiru eskritu ilustrativu mak di'ak tebes:

- Linguajen programasaun seguru memória (SSDF PW.6.1): Prioritiza ba uza linguajen programasaun seguru memória sé posivél. Ajênsia autorasaun rekoñese mitigasaun espesifiku memória sira seluk, hanesan randomizasaun layout espasu enderesu (ASLR), integridade fluksu kontrola (CFI) no fuzzing ne'e ajuda tebes ba baziku kodigu legadu, maibe la sufisiente atu haree nu'udar seguru-ho-dezeñu tanba sira la adekuadu atu prevene esplorasaun. Ezemplu balun husi linguajen seguru memoria, inklui C#, Rust, Ruby, Java, Go, no Swift. Lee iha information sheet seguransa memoria ba informasaun liutan.
- Baze Hardware Seguru: Inkorpora rekursu arkuitetura mak permite protesaun memória refinadu, hanesan deskreve ona ho Capability Hardware Enhanced RISC Instructions (CHERI) katak bele estende Instruction-Set Architectures (ISAs) hardware konvensional nian. Ba informasaun liutan vizita Universidade Cambridge CHERI webpage.
- Komponente Software Seguru (SSDF PW 4.1): Obten no mantein komponente software

mak seguru ho di'ak (p.e., biblioteka software nian, modulu sira, middleware, estrutura,) husi komersial verifikadu no dezenvolvedór parte terseiru nian atu garante seguransa robusta iha produtu software konsumidór nian.

- Estrutura modellu Web (SSDF PW.5.1): Uza estrutura modellu web mak implementa escape automatika husi input uzuáriu nian atu evita atake web sira hanesan script entre situs nian.
- Konsulta parametriza (SSDF PW 5.1): Uza konsulta parametriza duke inklui uzuáriu iha konsulta laran, atu evita atake injesaun SQL.
- Teste seguransa aplikativu estátiku no dinâmiku sira (SAST/DAST) (SSDF PW.7.2, PW.8.2): Uza ekipamentu sira ne'e atu analiza kodigu rekursu produtu nian no komportamentu aplikativu atu detekta pratika propensa erru sira. Feramenta sira ne'e taka problema sira husi jerensiamentu memória inadekuadu to'o kontrusaun konsulta banku dadus propensa erru (p.e., input uzuáriu sein escape no direta ba injesaun SQL). Feramenta SAST no DAST bele inkorpora ba prosesu dezenvolvimentu no opera automatikamente nu'udar parte husi dezenvolvimentu sofware nian. SAST no DAST tenke komplementa tipu teste seluk, hanesan teste unidade no teste integrasaun nian, atu garante produtu kumpri ho rekizitu seguransa mak espera ona. Kuandu problema identifika ona, fabrikante sira tenke realiza analize kauza prinsipál nian atu resolve vulnerabilidade sistematikamente.
- Revizaun kódigu (SSDF PW.7.1, PW.7.2): Esforsa atu garante katak kódigu submete tama produtu liuhosi revisaun kolega ho dezenvolvedór sira seluk atu garante kualidade aas liutan.
- Software Bill of Materials (SBOM) (SSDF PS.3.2, PW.4.1): Inkorpora kriasaun SBOM[3] atu fornese visibilidade tama ba konfigurasaun software mak hatama ba produtu sira.
- Programa divulgasaun vulnerabilidade (SSDF RV.1.3): Estabelese programa divulgasaun vulnerabilidade mak permite peskizadór seguransa ba relata vulnerabilidade sira no simu protesaun legal atu halo nune'e. Nu'udar parte husi ida ne'e, fornesedór sira tenke estabelese prosesu atu determina kauza prinsipál husi vulnerabilidade mak deskoberta ona. Prosesu ne'e tenke inklui determinasaun karik adota kualkér pratika Seguru-ho-Dezeñu husi dokumentu ida ne'e (ka pratika seluk mak hanesan) sei prevene introdusaun ba vulnerabilidade.
- Kompletude CVE: Garante katak CVE mak publika ona inklui hotu kauza prinsipál ka enumersaun frakeza komum (CWE) atu abilita analize industria luan liutan husi kauza prinsipál seguransa software nian. Embora garante katak kada CVE koretu no kompletu bele han tempu estra, ne'e permite diferente entidade atu tendensia industria mak fó

[3] Ajênsia autorasaun balun esplora hela abordajen alternativu atu obten garantia seguransa kona-ba kadeia fornesimentu software nian.

benefisiu ba fabrikante no kliente hotu-hotu. Ba informasaun liutan kona-ba jere vulnerabilidade, haree CISA's Stakeholder- specific SVCC guidance.

- Defesa iha Profundidade: Dezeña infraestrutura para kompromet imentu kontrola seguransa ida la impaktu ba kompromet imentu ba sistema tomak. Por ezemplu, garante katak priviléjiu uzuáriu nian provizionadu estritamente no lista kontrola asesu mak uza atu redus impaktu husi konta ida mak kompromet imentu ona. No mós, téknika sandboxing software bele kuarentena vulnerabilidade ba limita kompromet imentu husi aplikasaun tomak.

    - Kompletu Tarjetu Dezempeñu Sibernétiku sira (CPGs): Dezeña produtu mak hasoru pratika baziku seguransa nian. CISA's Cybersecurity Performance Goals esplika medidas fundamental bazika seguransa sibernétika organizasaun tenke implementa. Aleinde, ba maneira liutan atu fortifika Ita-nia organizasaun, haree ba UK's Cyber Assessment Framework ne'ebé fahe semellansa ba CISA's CPGs. Se fabrikante falta ba hasoru CPGs—hanesan la presija autentikasaun multifatór mak resistente ba empregadu hotu-hotu—depois sira labele konsidera ba fornese produtu mak Seguru-ho-Dezeñu nian.

Ajênsia autorasaun rekoñese katak mudansa sira ne'e mak tornu signifikadu iha postura organizasaun nian. Nune'e, sira-nia introdusaun tenke prioritiza bazeia ba kritikamente, kompleksidade no impaktu negosiu nian. Pratika sira ne'e bele introdus ba software foun no inkremental haluan atu taka kada kazu uza nian no produtu sira. Iha kazu balun, kritikamente no postura risku husi produtu sertamente karik persija kronograma aseleradu atu adota pratika hirak ne'e. Iha sira seluk, pratika bele introdus inkorpora ba baze kódigu legadu no korejiu iha tempu.

Tática Seguru-ho-Padraun sira

Aleinde atu adota pratika dezenvolvimentu Seguru-ho-Dezeñu, Ajênsia autorasaun rekomenda fabrikante software sira prioritiza konfigurasaun Seguru-ho-Padraun iha sira-nia produtu. Sira ne'e tenke esforsa atu atualiza produtu sira para akordu ho pratika sira ne'e kuandu sira ne'e atualizadu ona. Por Ezemplu:

- Elimina seña padraun sira: Produtu sira labele mai ho seña padraun mak fahe ona universalidade. Atu elimina seña padraun sira, Ajênsia autorasaun rekomenda produtu sira presija administradór atu konfigura seña forte durante instalasaun no konfigurasaun.
    - o Obriga Autentikasaun Multifatór (MFA) ba uzuáriu privilejiadu. Ami observa katak barak implantasaun empreza nian jere ho administradór sira mak ladauk proteje sira-nia konta ho MFA. Hanoin katak administradór sira hanesan tarjetu ho valór aas nian, produtu sira tenke halo MFA la partisipa duke partisipa. Aleinde, sistema tenke notifika regularmente ba administradór atu inskreva iha MFA to'o sira susesu abilita ida ne'e ba sira-nia konta. NCSC Olanda iha orientasaun paralela CISA nian, vizita

Mature Authentication Factsheet ba informasaun liutan.

- Logon úniku (SSO): Aplikasaun TI tenke implementa teknolojia logon úniku liuhosi padraun nakloke modernu. Ezemplu sira inklui Security Assertion Markup Language (SAML) ka OpenID Connect (OIDC.) Abilidade ida ne'e tenke halo disponivel ho padraun sein kusta adisional.
- Rejistru Seguru: Fornese logs auditoria ba kliente sira sein kusta adisional. Logs auditoria ne'e krusial atu detekta no eskala insidente seguransa potensial nian. Sira mós krusial durante investigasaun ida ba suspeitu ka insidenti seguransa mak konfirma ona. Konsidera pratika melloria hanesan fornese integrasaun fasil ho sistema informasaun seguransa no jerensiamentu eventu ho asesu aplikasaun programa superfisie (API) mak uza oras universal koordenadu (UTC), formatasaun orário estandar no téknika robusta dokumentasaun nian.
- Perfilu Autorizasaun Software: Fornesedór software tenke fornese rekomendasaun ba papél perfilu autorizadu nian no kazu uza mak sira designadu ona. Fabrikante sira tenke inklui avizu visivel mak notifika katak kliente sira husi risku mak aumenta se sira devia husi perfilu autorizasaun rekomenda ona. Por Ezemplu: Médiku sira bele visualiza ba rejistru pasiente hotu-hotu, maibe ajendador médiku ida iha asesu limitadu atu ba buka informasun mak presija ba ajendamentu konsulta nian.
- Seguransa haree ba futuru duke kompatibilidade anterior. Frekuentemente, rekursu legadu kompatível versaun anterior inkluí no dalaruma ativadu iha produtu nia laran mak hamosu risku ba seguransa produtu nian. Prioritiza seguransa duke kompatibilidade anterior, empoder ekipa seguransa atu hasai rekursu la seguru maski ida ne'e signifika ba kauza mudansa mak estraga.
- Rastreia no redus tamañu “guia enduresimentu”: Redus tamañu “guia enduresimentu” mak produs ba produtu sira no enforsa atu garante katak tamañu ne'e redus ona husi tempu ba tempu tanba software versaun foun publika ona. Integra komponente husi "guia enduresimentu" nian hanesan konfigurasaun padraun produtu nian. Ajênsia autorasaun rekoñese katak habadak guia enduresimentu ne'e rezultadu husi parseiru kontinua ho kliente mak iha no inklui forsa husi ekipa produtu barak, inklui esperiênsia uzuáriu (UX)
- Konsidera konsekuênsia esperiênsia uzuáriu husi konfigurasaun seguransa: Kada konfigurasaun foun aumenta todan kognitivu ba uzuáriu final no tenke avalia relasiona ho benefisiu komersial mak bele obten. Idealmente, konfigurasaun tenke la bele eziste, aleinde, konfigurasaun mak seguru tebes tenke integra tama ba produtu iha padraun. Kuandu konfigurasaun nesesariu, opsaun padraun tenke seguru haluan tan kontra ameasa komum.

Ajênsia autorasaun rekoñese mudansa hirak ne'e iha efeitu operasional ba oinsá software ne'e

hala’o. Entaun opiniaun kliente nian ne'e mak kritikal ba balansu operasional no konsiderasaun seguransa nian. Ajênsia autorasaun fiar katak roteiru eskrita nian no apoiu ezekutivu mak prioritiza ideia hirak ne'e inkorpora ba organizasaun nia produtu kritiku sira hanesan etapa primeiru atu muda ba pratika dezenvolvimentu software mak seguru. Maski opiniaun husi kliente ne'e importante, ajênsia autorasaun observa ona kazu importante sira, ne'ebé kliente sira lakohi ka labele adota padraun mak hadi'ak ona, dalaruma protokolu rede nian. Importante ba fabrikante sira atu kria insentivu signifikadu ba kliente sira atu mantein atualizadu no la permite sira permanente vulneravel indefinidamente.

GUIA BA ENDURESIMENTU VS AFRUKSAMENTU

Guia enduresimentu bele rezulta husi falta kontrola seguransa produtu mak inkorpora ba arkuitetura produtu husi dezenvolvimentu inisial. Konsekuentemente, guia enduresimentu mós bele sai roteiru eskrita ba adversáriu atu identifika no esplora rekursu mak la seguru. Komum ba organizasaun barak deskoñese guia enduresimentu, entaun sira husik tiha sira-nia ordenasaun konfigurasaun dispositivu iha postura la seguru ida. Modellu invertidu mak koñese nu'udar guia afruksamentu tenke troka guia enduresimentu no esplika mudansa ida ne'ebé uzuariu sira tenke halo embora mós lista rezultadu risku seguransa nian.

Duke dezenvolve guia enduresimentu mak lista métodu sira atu proteje produtu, ajênsia autorasaun rekomenda fabrikante software sira muda ba abordajen Seguru-ho-Padraun ho fornese guia afruksamentu ida. Orientasaun ida ne'e esplika risku husi dezisaun iha lingua simples, kompreensivel no bele levanta konsiente organizasional nian husi risku ba intruisaun sibernétika malisiozu sira. Kompensasaun seguransa tenke determina ho ezekutivu senior kliente nian, balansu seguransa ho rekizitu negosiu sira seluk.

REKOMENDASAUN HIRAK BA KLIENTE SIRA

Ajênsia autorasaun rekomenda organizasaun sira husu resonsabiliza fabrikante mak fornese teknolojia ba sira kona-ba rezultadu seguransa husi sira-nia produtu. Nu'udar parte husi ida ne'e, ajênsia autorasaun rekomenda katak ezekutivu organizasional prioritiza importansia ba sosa produtu seguru-ho-dezeñu no seguru-ho-padraun nian. Ida ne'e bele manifesta liuhosi estabelesimentu polítika ma tenkiser departementu TI asesus seguransa husi software fabrikante nian molok ba sosa, hanesan mós empoder departementu TI ba obrigda se nesesariu. Departementu TI sira tenke emporadu atu dezenvolve kritériu ba sosa nian mak enfaze importansia husi pratika Seguru-ho-Dezeñu no Seguru-ho-Padraun nian (sira ne'e esplika ona iha dokumentu ida ne'e no sira seluk mak dezenvolve ona ho organizasaun). Aleinde, departementu TI sira tenke apoiu ho jerensiamentu ezekutivu nian kuandu aplika kritériu sira ne'e iha dezisaun ba sosa nian. Dezisaun organizasional atu aseita risku mak asosiadu ho produtu teknolojia espesifiku nian tenke arkivu formalmente, aprovadu ho ezekutivu senior negosiu nian no regularmente aprezenta ba Konsellu Administrasaun.

Serbisu TI empreza prinsipál sira mak apoiu postura seguransa organizasaun nian, hanesan rede empreza, identidade empreza no asesu jerensiamentu, no operasaun seguransa nian no responde

kapasidade sira, tenke haree nu'udar funsaun negosiu kritiku hirak mak fundu ona atu aliña ho sira-nia importansia ba susesu misaun organizasaun nian. Organizasaun tenke dezenvolve planu ida atu hasa'e kapasidade hirak ne'e atu levanta fabrikante sira mak haku'ak pratika seguru-ho-dezeñu no seguru-ho-padraun.

Iha ne'ebé posivél, organizasaun tenke esforsa atu fortifika estratejia relasaun parseira ho sira-nia fornesedór TI. Relasaun hanesan ne'e inklui fiar iha nivel multipla sira husi organizasaun no fornese meius atu rezolve problema no identifika prioridade mak fahe hamutuk ona. Seguransa tenke sai elementu krítiku husi relasaun hanesan nune'e no organizasaun sira tenke esforsa atu reforsa importansia husi pratika Seguru-ho-Dezeñu no Seguru-ho-Padraun nian iha dimensaun formal (p.e., kontratu ka akordu fornesedór nian) no naun formal husi relasaun ne'e. Organizasaun tenke espera transparensia husi sira-nia fornesedór teknolojia kona-ba sira-nia postura kontrola interna no mós roteiru eskrita sira nian mak adota pratika Seguru-ho-Dezeñu no Seguru-ho-Padraun nian.

Aleinde, atu halo Seguru-ho-Padraun nu'udar prioridade iha organizasaun nia laran, lider TI sira tenke kolabora ho sira-nia kolega industria ba komprende produtu no serbisu ida ne'ebé mak di'ak tebes atu inkorpora prinsipiu dezeñu sira ne'e. Lider sira ne'e tenke koordena sira-nia pedidu atu ajuda fabrikante sira ba prioritiza sira-nia inisiativu seguransa tuir mai nian. Ho serbisu hamutuk, kliente sira bele ajuda fornese opiniaun signifikadu ba fabrikante no kria insentivu ba sira atu prioritiza seguransa.

Kuandu sira levanta sistema cloud nian, organizasaun tenke garante responsabilidade modellu mak fahe ona ho sira-nia fornesedór teknolojia. Ne'e katak organizasaun tenke klaru kona-ba responsabilidade seguransa fornesedór nian laos deit responsabilidade kliente nian. Organizasaun tenke prioritiza fornesedór cloud mak transparente kona-ba sira-nia postura seguransa, kontrola internal no kapasidade atu kumpri obrigasaun sira bazeia ba modellu responsabilidade mak fahe ona.

DESAPROVADÓR

Informasaun iha relatóriu ida ne'e, fornese "mak ne'e duni" ho objetivu fó informasaun deit. CISA no ajênsia autorasaun la apoiu kualkér produtu komersial ka serbisu, inklui kualkér objetu análize. Kualkér referência atu espesifiku entidade komersial ka produtu komersial nian, prosesu ka serbisu ho marka serbisu nian, marka komersial, fabrikante ka sira seluk tan, laos konstitui ka implika endossu, rekomendasaun ka favoritismu ho CISA no ajênsia autorasaun. Dokumentu ida ne'e hanesan inisiatiu konjuntu ho CISA ne'ebé la automatikamente serbi nu'udar dokumentu regulatoriu nian.

REKURSU SIRA

CISA

- CISA's SBOM Guidance
- CISA's Cross-Sector Cybersecurity Performance Goals
- Guidelines on Technology Interoperability
- CISA and NIST's Defending Against Software Supply Chain Attacks
- The Cost of Unsafe Technology and What We Can Do About It | CISA
- Stop Passing the Buck on Cybersecurity: Why Companies Must Build Safety Into Tech Products (foreignaffairs.com)
- CISA's Stakeholder-Specific Vulnerability Categorization (SSVC) Guidance
- CISA's Phishing Resistant MFA Fact Sheets
- Cyber Guidance for Small Businesses | CISA

NSA

- NSA's Cybersecurity Information Sheet on Memory Safety
- NSA's ESF Securing the Software Supply Chain: Best Practices for Suppliers FBI
- Understanding and Responding to the SolarWinds Supply Chain Attack: The Federal Perspective
- The Cyber Threat - Response and Reporting
- FBI's Cyber Strategy

Institutu Nasional Padraun no Teknolojia/National Institute of Standards and Technology (NIST)

- NIST's Digital Identity Guidelines
- NIST's Cyber Security Framework

NIST's Secure Software Development Framework (SSDF)

Sentru Australianu Seguransa Sibernétika/Australian Cyber

Security Centre (ACSC)

- ACSC's IoT Code of Practice Guidance for Manufacturers

The Sentru Nasional Seguransa Sibernétika Reinu

Unidu/United Kingdom's National Cyber Security Centre (UK)

- The UK's Cyber Assessment Framework
- The UK NCSC's Secure Development and Deployment guidance
- The UK NCSC's Vulnerability Management guidance
- The UK NCSC's Vulnerability Disclosure Toolkit
- University of Cambridge's CHERI
- So long and thanks for all the bits - NCSC.GOV.UK

Centro Kanadense Seguransa Sibernétika/Canadian

Centre for Cyber Security (CCS)

- CCCS's Guidance on Protecting Against Software Supply Chain Attacks
- Cyber supply chain: An approach to assessing risks
- Canadian Centre for Cyber Security's CONTI ransomware guidance

Escritóriu Federal Seguransa Informasau Alemanha/Germany's Federal

Office for Information Security (BSI)

- The BSI Grundschutz compendium (module CON.8)
- The international standard IEC 62443, part 4-1
- State of IT-security in Germany report, 2022
- BSI practices of web application security

Sentru Nasional Seguransa Sibernétika

Olanda/Netherlands' National Cyber Security

Centre

- NCSC-NL's Mature Authentication Factsheet

Seluk

- How Complex Systems Fail
- The New Look in complex system failure