TLP:CLEAR

Seftem Balens blong Saebasikiuriti Risk: Ol Prinsipol mo ol Aproj blong Sikiuriti-tru long-Disaen mo -Difolt

Pablikeisen: Eprel 13, 2023

Cybersecurity and Infrastructure Security Agency *(Saebasikiuriti mo Infrastrakja Sikiuriti Ejensi)*

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

Disklema: Dokumen ia oli makem TLP:KLIA. Disklosa hem i no limited. Ol sos maet oli save yusum TLP:KLIA taem we infomeisen hem i karem minimal o no risk blong misyus we man i save luk, folem ol rul mo prosija we oli aplae blong pablik rilis. Hem i sabjek long ol standed kopiraet rul, TLP: KLIA infomeisen oli save distributum witaot restriksen. Blong moa infomeisen abaot Trafik Laet Protokol, lukluk http://www.cisa.gov/tlp/.

Tebol blong ol Topik

OVAVIU: VALNEREBOL TRU LONG DISAEN

Teknoloji hem i stap insaed long klosap evri eria blong deili laef. Ol sistem we man i aksesem tru long intanet oli konek i ko long ol impoten sistem we oli afektem long wan daerek wei ikonomik prosperiti, laef, mo iven helt blong yumi, mo hemia i inkludim pesenal aedentiti manejmen kasem medikol kea. Olsem wan eksampol nomo, ol saeba atak i bin mekem se ol hospital oli kanselem ol sejeri mo daevetem kea blong ol peisen raon long wol. Taem teknoloji i no sikiua mo ol impoten sistem oli isi blong atakem, hemia i save invaetem ol rabis saeba atak, we maet i save mekem se i stap kat ol siries sefti[1] risk.

Naoia bitim bifo, hem i impoten blong ol teknoloji manufakjera oli mekem Sikiua-tru long-Disaen mo Sikiua tru long Difolt ol mein poen blong prodak disaen mo ol divelopmen proses. Sam venda oli bin tekem ol bigfala step blong draevem indastri ia i ko fowod long sofwea asurens, be ol narafala wan oli bihaen. Ol ejensi we oli raetem buk ia oli stap enkarejem long wan strong wei evri teknoloji manufakjera blong bildim ol prodak blong olketa long wan wei we i mekem se ol kastoma oltaem oli no nid blong mekem monita, ol rutin apdeit, mo damej kontrol long ol sistem blong olketa blong mekem se ol saeba atak oli no hapen tumas. Oli stap enkarejem ol manufakjera blong oli tekem onasip blong impruvum ol sikiuriti aotkam blong ol kastoma blong olketa. Folem histri, ol teknoloji manufakjera oli bin stap dipen long fasin blong fiksim ol ples we i isi blong oli atakem we oli faenem afta we ol kastoma oli instolem ol prodak, mo hem i nidim ol kastoma blong oli yusum mani blong olketa wan blong fiksim ol eria ia. Sipos nomo we yumi yusum ol Sikiua-tru long-Disaen praktis bambae yumi brekem ol rabis saekol blong krietem mo aplaem ol ansa mo aplaem olketa.

Blong kasem hae standed blong sofwea sikiuriti ia, ol ejensi we oli raetem buk ia oli stap enkarejem ol manufakjera blong putum olsem praeoriti intekreisen blong prodak sikiuriti olsem wan impoten pririkwisit long ol fija mo spid from maket. Ova taem, ol tim blong ol enjinia bambae oli save putum wan niu peis we i stap semak oltaem we sikiuriti hem i rili disaen insaed mo i tekem les wok blong mentenem.

Yuropian Yunion hem i riflektem tingting ia, taem hem i riinfosem impotens blong prodak sikiuriti long Cyber-Resilience-Act (Saeba Risiliens Akt), we i emfasaesem se ol manufakjera oli mas implementem sikiuriti truaot long laef saekol blong wan prodak blong stopem ol manufakjera blong oli no intodusum ol prodak i ko long maket we maet oli isi blong atakem.

Blong krietem wan fiuja we teknoloji mo ol prodak we oli yusum teknoloji oli sef blong ol kastoma, ol ejensi we oli raetem buk ia oli askem ol manufakjera blong oli jenjem disaen blong olketa mo divelopem ol prokram blong oli alaoem Sikiua-tru long-Disaen mo ol Difolt prodak blong oli shipim i ko long ol kastoma. Ol prodak

[1] Ol ejensi we oli raetem buk ia oli luksave se wod ia "sefti" hem i kat fulap mining we i folem konteks we man i yusum long hem. Folem pepes blong gaed ia, "sefti" bambae hem i rifea long fasin blong leftemap ol standed blong teknoloji sikiuriti blong protektem ol kastoma long ol rabis saeba aktiviti.

we oli Sikiua-tru long-Disaen oli olketa we sikiuriti blong ol kastoma hem i mein bisnis eim, mo hem i no jes wan teknikol fija. Ol prodak we oli Sikiua-tru long-Disaen oli stat wetem eim ia bifo divelopmen hem i stat. Ol prodak we oli Sikiua-tru long-Disaen oli olketa we oli sikiua blong yusum 'aotsaed long boks' wetem smol o nokat konfikureisen jenj we i neseseri mo oli kat ol sikiuriti fija we i nokat adisenal kost blong hem.

Tuketa, tufala prinsipol ia oli muvum bigfala pat blong beden blong stap sikiua i ko long ol manufakjera mo i katem daon ol janis se ol kastoma bae oli kam viktim blong ol sikiuriti insiden we i hapen from ol miskonfikureisen, kwik ripea wok we i no naf, o fulap narafala isiu we i komon.

Cybersecurity and Infrastructure Security Agency (CISA) (*Saebasikiuriti mo Infrakstrakja Sikiuriti Ejensi)*, National Security Agency (NSA) *(Nasonal Sikiuriti Ejensi)*, Federal Bureau of Investigation (FBI) *(Federel Byuro blong Investikeisen)* mo olketa intanasonal patna ia[2] oli stap kivim ol rekomendeisen insaed long gaed ia olsem wan rodmap blong teknoloji manufakjera blong mekem sua se i kat sikiuriti blong ol prodak blong olketa:

- Australian Cyber Security Centre (ACSC)
- Canadian Centre for Cyber Security (CCCS)
- United Kingdom's National Cyber Security Centre (NCSC-UK)
- Germany's Federal Office for Information Security (BSI)
- Netherlands' National Cyber Security Centre (NCSC-NL)
- Computer Emergency Response Team New Zealand (CERT NZ) mo New Zealand's National Cyber Security Centre (NCSC-NZ).

Ol ejensi we oli raetem buk ia oli luksave ol kontribusen blong fulap praevet sekta patna blong mekem sikiuriti-tru long-disaen mo sikiuriti-tru long-difolt hem i muv fowod. Eim blong prodak ia hem i blong muvum wan intanasonal konveseisen abaot ol mein praeoriti, ol invesmen, mo ol disisen blong ajivim wan fiuja we teknoloji hem i sef, sikiua, mo risilien tru long disaen mo difolt. Blong kasem eim ia, ol ejensi we oli raetem buk ia oli askem ol pati we oli intres blong kivim fidbak long prodak ia mo oli wantem kat wan siris blong ol sesen we bae oli lisen blong jenjem moa, spesifaem mo advansem gaedans blong yumi blong ajivim ol gol we yumi sherem.

Blong kasem moa infomeisen abaot impotens blong prodak sefti, lukluk atikol blong CISA, The Cost of Unsafe

[2] Afta long ples ia oli rifea long hem olsem "ol ejensi we oli raetem buk ia."

Technology and What We Can Do About It *(Kos blong Teknoloji we i no Sef mo Wanem we Yumi Save Mekem Abaotem)*.

Sikiua-tru long-Disaen

"Sikiua-tru long-Disaen" hem i minim se oli bildim ol teknoloji prodak long wan wei we hem i stopem long wan risinabol wei ol rabis saeba akta blong oli kat sakses taem oli aksesem ol divaes, data, mo infrastrakja we i konek. Ol sofwea manufakjera oli mas mekem wan risk asesmen blong aedentifaem mo nambarem ol saeba tret we oli stap ko raon long ol mein sistem, mo afta inkludim ol proteksen long ol prodak bluprint we i eksplenem saeba tret landskep we i stap jenj.

Mifala i rekomendem tu ol divelopmen praktis blong sikiua infomeisen teknoloji (IT) mo ol maltipol leia difens – we oli kolem dip-difens – blong stopem aktiviti blong ol ataka blong i ko putum ol sistem long denja o blong oli aksesem sensitif infomeisen we oli no sapos blong aksesem. Ol ejensi we oli raetem buk ia oli rekomendem se ol manufakjera oli yusum wan tret model we oli mekem long taem blong divelopmen blong prodak blong adresem evri potensel tret long wan sistem mo eksplenem wanwan diploemen proses.

Ol ejensi we oli raetem buk ia oli askem ol manufakjera blong tekem wan ful sikiuriti aproj blong ol prodak mo platfom blong olketa. Sikiua-tru long-Disaen divelopmen hem i nidim se ol sofwea manufakjera oli investem bigfala risos long wanwan leia blong prodak disaen mo divelopmen proses we bae oli no save "putum i ko" afta. Hem i nidim strong lidasip long ol top bisnis eksekiutif blong manufakjera blong mekem sikiuriti wan bisnis preoriti, mo i no se hem i jes wan teknikel fija nomo. Kolaboreisen ia bitwin ol bisnis lida mo ol teknikol tim hem i eksten long ol eli stej blong disaen mo divelopmen, tru long kastoma diploemen mo mentenens. Oli enkarejem ol manufakjera blong mekem ol had tredof mo ol invesmen, inkludim olketa we bambae oli "invisibol" long ol kastoma, olsem wok blong kamaot mo ko long ol prokraming langwij we oli waepemaot ol wiknes. Oli shud praeoritaesem ol fija, ol mekanisim, mo implimenteisen blong ol tul we oli protektem ol kastoma kompea long wok blong praeoritaesem ol fija we maet i luk gud be i mekem atak sefes i bigwan.

I nokat wan singol ansa blong endem tret we i stap oltaem blong ol rabis saeba akta we oli tek advantej long ol wiknes insaed long teknoloji, mo ol prodak we oli "Sikiua-tru long –Disaen bambae oli kontinu blong safa long ol wiknes ia; be, wan bigfala set blong ol wiknes hem i from wan smol sabset blong ol rut kos. Ol manufakjera oli mas divelopem ol rodmap we oli raetem blong alaenem ol prodak potfolio blong olketa we oli stap naoia wetem moa Sikiua-tru long-Disaen praktis, mo mekem sua se oli folem wan difren rod taem nomo we i kat ol ekstraodineri situeisen.

Ol ejensi we oli raetem buk ia oli andastanem se fasin blong tekem onasip abaot ol sikiuriti aotkam blong ol

kastoma mo blong mekem sua se level blong kastoma sikiuriti ia maet bae save inkrisim ol divelopmen kost. Be, sipos ol manufakjera oli inves long ol "Sikiua-tru long-Disaen" praktis taem oli stap divelopem ol niufala teknoloji prodak mo mentenem olketa we oli stap finis, hemia hem i save impruvum bigwan sikiuriti blong ol kastoma mo katem daon janis blong ol ataka oli atak. Ol prinsipol blong Sikiua-tru long-Disaen oli no mekem sikiuriti blong ol kastoma i strong mo oli no mekem reputeisen blong brand hem i strong nomo be hem i katem daon mentenens mo pajing kos blong ol manufakjera long longtem.

Ol Rekomendeisen blong ol Sofwea Manufakjera seksen we oli listim i stap andanit ia hem i kivim wan list blong ol praktis mo polisi blong ol prodak divelopmen we oli rekomendem blong ol manufakjera oli tingbaot.

Sikiua-tru long-Difolt

"Sikiua-tru long-Difolt" hem i minim se ol prodak oli resilien akensem ol eksploiteisen teknik aotsaed long boks mo i no nidim adisenal kost. Ol prodak ia oli protek akensem ol tret mo ol wiknes we oli stap hapen oltaem mo ol en yusa oli no nid blong tekem ol ekstra step blong sikiurem olketa. Ol Sikiua-tru long-Difolt prodak oli disaenem blong mekem ol kastoma oli save gud se taem we oli ko aot long ol sef difolt, oli stap inkrisim ol janis blong oli stap long denja be sipos nomo we oli implementem ol ekstra kontrol we oli kompensetem wok ia.

- Wan sikiua konfikureisen i mas difolt beislaen. Ol prodak we oli Sikiua-tru long-Difolt oli tanem on ol mos impoten sikiuriti kontrol we yusa i nidim blong protektem ol bisnis akensem ol rabis saeba akta, mo tu blong kivim paoa blong yusum mo konfigarem moa ol sikiuriti kontrol be i nomo nid blong pem ekstra kos.
- Kompleksiti blong sikiuriti konfikureisen hem i no shud stap olsem wan kastoma problem. Ol IT staf blong ol okanaeseisen sam taem oli ova lod wetem ol sikiuriti mo opereisenal risponsibiliti, mekem se oli nokat inaf taem blong andastanem mo implementem ol sikiuriti implikeisen mo mitikeisen we oli nidim blong kat wan strong saeba sikiuriti. Taem ol manufakjera oli impruvum sikiua prodak konfikureisen—sikiurem "difolt rod" —oli save helpem ol kastoma blong olketa taem oli mekem sua se oli manufakjarem, distributum mo yusum long sikiua wei folem ol standed blong "Sikiuriti-tru long-Difolt".

Ol manufakjera blong ol prodak we oli "Sikiua-tru long-difolt oli no jajem wan ekstra kos blong implimentem ol ekstra sikiuriti konfikureisen. Be, oli inkludim olketa insaed long beis prodak olsem ol sitbel we oli inkludim insaed long evri niu trak. Sikiuriti hem i no wan lakseri opsen be hem i moa klosap long standed we evri kastoma oli mas ekspektem we oli no nikosiet from o pem moa from.

OL REKOMENDEISEN BLONG OL SOFWEA MANUFAKJERA

Joen gaed ia hem i kivim ol rekomendeisen i ko long ol manufakjera blong divelopem wan rodmap we oli raetem blong implementem mo mekem sua se i kat IT sikiuriti. Ol ejensi we oli raetem buk ia oli rekomendem se ol sofwea manufakjera oli implementem ol strateji mo aotlaenem long ol seksen andanit ia blong tekem onasip blong ol sikiuriti aotkam blong ol kastoma blong olketa tru long ol prinsipol blong Sikiua-tru long-Disaen mo -Difolt.

Ol Prinsipol blong Sofwea Prodak Sikiuriti

Mifala i stap enkarejem ol teknoloji manufakjera blong adoptem wan stratejik fokas we i praeoritaesem sofwea sikiuriti. Ol ejensi we oli divelopem ol trifala impoten prinsipol ia andanit ia blong gaedem ol sofwea manufakjera blong bildim sofwea sikiuriti i ko insaed long ol disaen proses blong olketa bifo oli divelopem, konfikurem mo shipim ol prodak blong olketa.

1. Beden blong sikiuriti i no shud foldaon fulwan long kastoma. Ol sofwea manufakjera oli mas tekem onaship long ol sikiuriti aotkam blong pejes blong kastoma blong olketa mo from risen ia oli mas jenjem ol prodak blong olketa.
2. Holem radikol transparensi mo akaontebiliti. Ol sofwea manufakjera oli shud tekemap radikol transparensi mo akaontebiliti. Ol sofwea manufakjera oli shud leftemap olketa wan blong dilivarem ol sef mo sikiua prodak, mo tu blong difrensietem olketa wan aot long evri narafala wan insaed long manufakjera komuniti folem abiliti blong olketa wan blong mekem hemia. Hemia hem i inkludim fasin blong serem infomeisen we oli lanem long ol kastoma diploemen blong olketa, olsem oli apruvum ol strong otentikeisen mekanisim tru long difolt. Hem i inkludim tu wan strong komitmen blong mekem sua se ol rikod blong ol advaes abaot ol risk mo ol komon risk mo eksposa (CRE) oli komplit mo stret. Be, lukaot long temteisen blong kaontem ol CRE olsem wan neketif metrik, from se ol kaen namba olsem oli wan saen tu blong wan helti kod analisis mo testing komuniti.
3. Bildim wan okanaeseisenal strakja mo lidaship blong ajivim ol gol ia. No mata we ol sabjek mata ekspetis hem i impoten long prodak sikiuriti, ol sinia eksekiutif oli ol praemeri disisen meka blong implementem jenj long wan okanaeseisen. Eksikiutif-level komitmen blong ol sofwea manufakjera blong praeoritaesem sikiuriti olsem wan kritikol elemen blong prodak divelopmen hem i nidim divelopmen blong ol patnaship wetem ol kastoma blong wan okannaeseisen blong andstanem:
    a. Prodak diploemen sinario gaedans wetem tret model we i stret

b. Implimenteisen blong ol sikiuriti kontrol we oli proposem blong i folem ol prinsipol blong Sikiua-tru long-Difolt.

c. Ol risos alokeisen strateji we oli mekem blong folem kampani saes mo abiliti blong riplesem ol lekasi divelopmen praktis wetem ol praktis blong Sikiua-tru long-Disaen.

d. Nid blong mentenem wan open laen blong komunikeisen blong intenal mo ekstenam fidbak (eksampol, employi mo kastoma fidbak) abaot ol isiu blong prodak sikiuriti. Oli mas emfasaesem sofwea sikiuriti insaed long ol intenal forom (eksampol, ol kampani waed miting mo ol infomol miting), mo tu ol ekstenel prodak maketing mo kastoma engeijmen

e. Ol mesamen blong ifektifnes insaed long ol kastoma diploemen. Ol sinia eksekiutif lida oli wantem save weaples ol invesmen long sikiuriti tru long disaen mo difolt oli stap helpem ol kastoma taem oli sloem peis long ol sikiuriti paj, katem daon ol konfikureisen mistek, mo minimaesem sefes atak.

Blong mekem olketa trifala prinsipol ia, ol manufakjera oli shud tingbaot sam opereisenal taktik blong jenjem ol divelopmen proses blong olketa.

Holem ol rutin miting wetem kampani eksekiutif lidaship blong draevem impotens blong Sikiua-tru long Disaen insaed long okanaeseisen. Oli mas establishim ol polisi mo ol prosija blong riwodem ol prodaksen tim we oli stap divelopem ol prodak blong folem ol prinsipol ia, we i save inkludim ol awod blong implementem aotstanding sofwea sikiuriti praktis o ol insentif blong wok lada mo promosen kraeteria.

Opereit raon long impotens blong sofwea sikiuriti long bisnis sakses. Eksampol, tingting blong putum wan “sofwea sikiuriti lida” o wan “sofwea sikiuriti tim” we i holem ol bisnis mo IT praktis blong i joenem ol sikiuriti standed mo manufakjera akaontebiliti. Ol manufakjera oli mas mekem sua se oli kat wan strong, indipenden prodak sikiuriti asesmen mo ol ivalueisen prokram blong ol prodak blong olketa.

Yusum wan tret model we oli mekem long taem blong divelopmen blong praeoritaesem ol prodak we oli mos impoten mo oli kat hae impak. Ol tret model oli tingbaot wan speifik yus-keis blong wan prodak mo mekem sua se ol divelopmen tim oli sikiurem ol prodak. Las wan, sinia lidaship i shud holem ol tim oli akaontebol blong dilivarem ol sikiua prodak olsem wan mein elemen blong prodak ekselens mo kwaliti.

Ol Taktik blong Sikiua-tru long-Disaen

Sikiua Sofwea Divelopmen Fremwok (SSDF), we oli save tu olsem Nsonal Institut blong ol Standed mo Teknoloji (NIST) SP 800-218, hem i wan mein set blong ol hae level sikiua sofwea divelopmen praktis we oli save putum i ko insaed long wan wan stej blong sofwea divelopmen laefsaekol (SDLS). Taem ol sofwea produsa oli folem ol praktis ia hem i save helpem olketa blong oli kam moa ifektif blong faenem mo karemaot ol risk long ol sofwea we oli rilisim, katemdaon potensel ifek blong eksploitem ol risk, mo adresem ol rut kos blong ol risk blong stopem blong oli nomo hapen long fiuja.

Ol ejensi we oli stap raetem buk ia oli stap enkarejem yus blong ol taktik blong Sikiua-tru long Disaen, inkludim ol prinsipol we oli rifea long ol SSDF praktis. Ol sofwea manufakjera oli shud divelopem wan rodmap we oli raetem blong adoptem moa Sikiua-tru long Disaen sofwea divelopmen praktis akros long potfolio blong olketa. Lis ia hem i wan lis we i no komplit we i soem eksmapol blong rodmap blong ol bes praktis:

- Ol langwij blong memori sef prokraming (SSDF.6.1): Preoritaesem yus blong ol memori sef langwij weaples we i posibol. Ol ejensi we oli raetem buk ia oli luksave se ol narafala memori spesifikeisen mitikeisen, olsem adres speis leiaot randomaeseisen (ASLR), kontrol-flo intekriti (KFI), mo fasing oli helpful blong ol lekasi kodbes, be oli no inaf blong man i luk olsem sikiua-tru long-disaen from se oli nokat inaf eksampol blong stopem eksploiteisen. Sam eksampol blong moden memori sef langwij oli inlkudim C#, Rust, Rudy, Java, Go, mo Swift. Ridim memori sefti information sheet blong moa infomeisen.
- Sikiua Hadwea Faondeisen: Inkoporeitem ol akitek fija we i mekem sua se i kat memori proteksen we i stret long evri smol wei, olsem olketa ia we Capability Hardware Enhanced RISC Instructions (CHERI) hem i diskraebem we oli save ekstendem conventional hardware Instruction-Set Architectures (ISAs). Blong kasem moa infomeisen visitim CHERI webpage we hem i websaet blong Yunivesiti blong Kambridj.
- Ol Sikiua Sofwea Komponen (SSDF PW4.1): Akwaerem mo mentenem ol sofwea komponen we oli sikiua gud (eksampol, ol sofwea laebri, ol modul, midelwea, mo ol fremwok) long ol komesel, open sos, mo narafala ted pati divelopa we oli verifaem olketa blong mekem sua se i kat strong sikiuriti long ol konsuma prodak.
- Ol web templet fremwok (SSDF PW.5.1): Yusum ol web templet fremwok we i implementem otomatik eskeping blong yusa input blong kamaot long rod blong ol web atak olsem kros-saet skripting.

- Ol paramitaraes kweri (SSDF PW 5.1): Yusum ol paramitaraes kweri insted blong inludim yusa input insaed long ol kweri, blong kamaot long rod blong ol SQL injeksen atak.
- Statik mo daenamik aplikeisen sikiuriti testing (SAST/DAST) (SSDF PW.7.2, PW.8.2):
- Yusum ol tul ia blong analaesem prodak sos kod mo implikeisen biheivia blong ditektem ol praktis we oli ditektem ol praktis we oli save mekem mistek. Ol tul ia oli kavremap ol isiu we i stat long manejmen blong memori we i no stret i ko kasem konstraksen blong databeis kweri we i save kat mistek long hem (eksampol, yusa input we i no eskep we i lid i ko long SQL injeksen). Ol SAST mo ol DAST tul oli save inkoporetem i ko insaed long ol divelopmen proses mo ran otomatik olsem pat blong wan sofwea divelopmen. SAST mo DAST oli shud komplimentem ol narafala kaen testing, olsem unit testing mo intekreisen testing, blong mekem sua se ol prodak oli folem ol sikiuriti rikwaemen we oli ekspektem. Taem ol isiu ia oli aedentifaem, ol manufakjera oli mas mekem wan rut-kos analisis blong adresem ol risk long wan sistematik wei.
- Kod riviu (SSDF PW.7.1, PW.7.2): Traem blong meken sua se kod we divelopa i sabmitim i ko long ol prodak ia, ol narafala divelopa oli riviuem blong mekem sua se kwaliti hem i moa hae.
- Software Bill of Materials (SBOM) (SSDF PS.3.2, PW.4.1): Inkoporetem krieisen blong SBOM[3] blong kivim visibility i ko long wan set blong ol sofwea we i ko insaed long ol prodak.
- Ol valnarabiliti disklosa prokram (SSDF RV.1.3): Establishim ol valnaribiliti disklosa prokram we i alaoem ol sikiuriti riseja blong ripotem ol valnaribiliti mo risivim likol sef haba taem oli stap mekem hemia. Olsem wan pat blong hemia, ol saplaea oli mas establishim ol proses blong wokemaot ol rut kos blong ol valnaribiliti we oli diskaverem. Ol kaen proses ia oli mas inkludim wok blong wokemaot sipos we oli bin adoptem eni long ol Sikiua-tru long-Disaen praktis insaed long dokumen ia (o ol narafala semak praktis) bambae hem i stopem introdaksem blong valnaribiliti.
- Komplitnes blong CVE: Mekem sua se ol CVE we oli pablishim oli inkludim ol rut kos o komon wiknes enumereisen (CWE) blong mekem sua se i kat analisis we hem i tek ples long ful indastri blong ol rut kos blong sofwea sikiuriti. Taem wok blong mekem sua se evri CVE hem i stret mo komplit hem i save tekem ekstra taem, hem i alaoem ol entiti we oli no rilet blong spotem ol muvmen blong indastri we oli benefitim evri manufakjera mo ol kastoma. Blong moa infomeisen

[3] Sam long ol ejensi we oli raetem buk ia oli stap eksplorem ol narafala aproj blong aksesem ol sikiuriti asurens araon long sofwea saplae jein.

abaot wok blong manejem ol valnarabiliti, lukluk CISA's Stakeholder- specific SVCC guidance.

- Dip-Difens: Disaenem infrasktrakja blong mekem se kompromaes blong wan singol sikiuriti hem i no mekem se bae kat kompromaes blong ful sistem. Eksampol, taem divelopa hem i mekem sua se ol privilej blong yusa oli naro mo i yusum ol akses kontro lis, hemia i save katem daon impak blong wan akaon we i save stap long risk. Mo tu, ol teknik blong sofwea sanboksing oli save kwarantinim wan valnerabiliti blong limitim kompromaes blong wan ful aplikeisen.
- Satifaem ol Saeba Pefomens Gol: Disaenem ol prodak we oli mitim ol besik sikiuriti praktis. CISA's Cybersecurity Performance Goals *(Ol Saebasikiuriti Pefomens Gol blong CISA)* hem i aotlaenem ol mein, beislaen saebasikiuriti mesa we ol okanaeseisen oli mas implementem. Mo tu, blong kat moa wei blong strengtenem standing blong okanaeseisen blong yu, lukluk UK's Cyber Assessment Framework *(Saeba Asesmen Fremwok blong UK)* we hem i serem ol semak samting wetem ol CPG blong CISA. Sipos wan manufakjera hem i no mitim ol CPG—olsem hem i no mekem se i mas kat fishing-resisten malti-fakta otentikeisen blong evri employi—bambae oli no save luk olketa se oli stap dilivarem ol prodak we oli Sikiua-tru long-Disaen.

Ol ejensi we oli raetem buk ia oli luksave se ol jenj ia oli ol bigfala jenj insaed long weaples okanaeseisen i stap long hem. From hemia, oli mas praeoritaesem introdaksen blong olketa folem kritikaliti, kompleksiti mo bisnis impak. Oli save introdusum ol praktis ia blong niufala sofwea mo ekspandem long ol rekula stej blo kavremap ol keis mo ol prodak we oli ekstra. Long sam keis, kritikaliti mo risk ples blong wan seten prodak i save minim wan taemlaen we i hariap blong adoptem ol praktis ia. Long ol narafala keis, ol divelopa oli save introdusum ol praktis ia i ko insaed long wan lekasi kodbes mo risolvem bakegen ova long taem.

Ol taktik blong Sikiua-tru long-Difolt

Andap moa long wok blong adoptem ol divelopmen praktis blong Sikiua-tru long-Disaen, ol ejensi we oli raetem buk ia oli rekomendem se ol sofwea manufakjera oli praeoritaesem ol Sikiua-tru long-Difolt konfikureisen insaed long ol prodak blong olketa. Oli mas trae had blong apdeitem ol prodak blong olketa blong oli folem ol praktis ia taem oli rifreshem olketa. Eksampol:

- Elimineitem ol difolt paswod: Ol prodak oli no mas kam wetem ol difolt paswod we oli sherem long evri ples. Blong elimineitem ol difolt paswod, ol ejensi we oli raetem buk ia oli rekomendem prodak ia oli nidim ol administreta blong setem wan strong paswod long taem blong instoleisen mo konfikureisen.
    - Mandeitem Maltifakta Otentifikeisen (MFA) blong ol privilej yusa. Yumi luk se ol administreta

we oli manejem fulap entapraes diploemen oli no protektem ol akaon blong olketa wetem MFO. From se ol administreta oli ol hae valiu taket, ol prodak oli shud mekem MFO i jus blong no tekpat be i no jus blong tek pat. Andap long hemia, sistem i shud promptem long wan rekula wei administreta blong enrol long MFO kasem taem we oli kat sakses blong onem long ol akaon blong olketa. NCSC blong Netaland hem i kat gaedens we i semak olsem hemia blong CISA, visitim Mature Authentication Factsheet blong moa infomeisen.

- Singol saen-on (SSO): Ol IT aplikeisen oli mas implimentem singol saen on long teknoloji tru long ol moden open standed. Ol eksampol oli inkludim Sikiuriti Asesen Makap Langwij (SAML) o OpenID Connect (OIDC.) Kapabiliti ia i shud avelebol tru long difolt mo i no nid blong kat ekstra kost.
- Sikiua Loking: Provaedem hae-kwaliti odit lok i ko long ol kastoma mo nokat ekstra kos blong hemia. Ol odit lok oli impoten blong ditektem mo spidim ol potensel sikiuriti insiden. Tingbaot ol bes praktis olsem wok blong provaedem isi intekreisen wetem sikiuriti infomeisen mo o liven manejmen sistem (SIIM) wetem aplikeisen prokraming aplikeisen (API) akses we i yusum koodinet yunivesel taem (UTC), standed taem son fomating, mo ol strong dokumenteisen teknik.
- Sofwea Otoraeseisen Profael: Ol sofwea saplaea oli mas provaedem ol rekomendeisen long ol otoraes profael rol mo ol yus keis we oli desikneitem long olketa. Ol manufakjera oli mas inkludim wan visibol woning we i notifaem ol kastoma abaot wan risk we i bigwan sipos oli ko aot long profael otoraeseisen we oli rekomendem. Eksampol: ol medikol dokta oli save luk evri peisen rikod, be wan medikol woka we i stap mekem ol apoenmen hem i kat smol akses nomo blong adresem infomeisen we oli nidim blong mekem apoenmen.
- Sikiuriti we i lukluk fowod ova long kompatibiliti we i lukluk i ko bak: Fulap taem, ol lekasi fija we i ko bakwod oli stap insaed, mo samtaem oli tanem olketa fija ia i on nomata we oli mekem ol risk long sikiuriti blong prodak. Praeoritaesem sikiuriti ova long bakwod kompatibiliti, mo kivim paoa long ol sikiuriti tim blong karemaot ol fija we i nokat sikiuriti nomata sipos hemia i minim se bambae oli brekem ol jenj.
- Trakem mo katem daon “hadening gaed’ saes: Katem daon saes blong ol “hadening gaed” we oli produsum blong ol prodak mo traem blong mekem sua se saes i ko daon ova taem taem ol niu vesen blong sofwea oli rilis. Intekretem ol komponen blong “hadening gaed” ia olsem difolt konfikureisen blong prodak ia. Ol ejensi we oli raetem buk ia oli luksave se ol hadening gaed we oli sot oli risal blong patnaship we i stap kontinu wetem ol kastoma we oli stap mo oli inkludim ol efot blong fulap prodak tim, inkludim yusa eksperiens (UX).

- Tingbaot ol konsikwens blong yusa eksperiens blong ol sikiuriti seting: Wanwan niufala seting hem i inkrisim kognitif beden long ol en yusa mo oli shud asesem wetem bisnis benefit blong draevem. Bambae hem i moa gud se wan seting bae i nokat; be, seting we i moa sikiua bambae hem i mas intekret i ko insaed long prodak tru long difolt. Taem konfikureisen hem i neseseri, difolt opsen bambae i mas sikiua long wan jenerol wei akensem ol komon tret.

Ol ejensi we oli raetem buk ia oli luksave se ol jenj oli save kat ol ifek long opereisen blong hao kastoma i yusum sofwea ia. Mekem se, input blong kastoma hem i impoten blong balensem ol opereisenal mo sikiuriti konsidereisen. Ol ejensi we oli raetem buk ia oli biliv se ol rodmap we oli raetem mo eksekiutif sapot we hem i praeoritaesem olketa tingting ia i ko long ol mos kritikol prodak blong wan okanaeseisen hem i fesfala step blong jenj i ko long ol sikiua sofwea divelopmen praktis. Taem kastoma input hem i impoten, ol ejensi we oli raetem buk ia oli bin luk ol impoten keis we ol kastoma oli no bin wiling o oli no save adoptem ol impruv standed, samaem ol netwok protocol. Hem i impoten blong ol manufakjera oli krietem ol miningful insentif blong ol kastoma oli stap long presen mo no letem olketa blong oli stap valnerebol blong longtaem.

OL HADENING vs LUSENING GAED

Ol hadening gaed oli save kamaot from se i nokat ol sikiuriti kontrol we oli putum insaed long akitekja blong wan prodak long stat blong divelopmen. Mekem se, ol hadening gaed ia oli save olsem wan rodmap blong ol enemi blong pinpoenem mo eksploitem ol fija we oli nokat sikiuriti. Hem i komon blong fulap okanaeseisen se oli no awea long ol hadening gaed, mekem se oli leko ol divaes konfikureisen seting blong olketa long wan posisen we i no sikiua. Wan model we hem i invet we oli singaotem wan lusening gaed i mas riplesem ol hadening gaed mo eksplenem ol wanem jenj we ol yusa oli mas mekem taem oli stap listim ol sikiuriti risk we i kamaot long hemia.

Insted blong divelopem ol hadening gaed we i listim ol wei blong sikiurem ol prodak, ol ejensi we oli raetem buk ia oli rekomendem ol manufakjera blong jenj i ko long wan Sikiua-tru long-Difolt aproj tru long ol lusening gaed. Ol gaed ia oli eksplenem bisnis risk blong ol disisen long simpol, langwij we man i save andastanem, mo oli save reisem okanaeseisenal aweanes blong ol risk blong ol saeba intrusen. Ol sinia eksekiutif blong ol kastoma oli mas putum ol sikiuriti tredof, mo balensem sikiuriti wetem ol narafala bisnis rikwaemen.

OL REKOMENDEISEN BLONG OL KASTOMA

Ol ejensi we oli raetem buk ia oli holem ol manufakjera we oli saplaem teknoloji long olketa oli akaontebol blong ol sikiuriti aotkam blong ol prodak blong olketa. Olsem pat blong hemia, ol ejensi we oli raetem buk ia oli rekomendem se ol eksekiutif blong okanaeseisen oli praorataesem blong pem ol Sikiua-tru long-Disaen

mo ol Sikiua-tri long-Difolt prodak. Hemia i save kam tru long ol polisi we oli establishim we i nidim se ol IT dipatmen oli asesem sikiuriti blong manufakjera sofwea bifo oli pem, mo tu blong kivim paoa i ko long ol IT dipatmen blong pusum bak sipos i neseseri. Ol IT dipatmen oli mas kat paoa blong divelopem kraeteria blong pem samting we i emfasaesem impotens blong ol praktis blong Sikiua-tru long-Disaen mo Sikiua-tru long-Difolt (tuketa olketa we oli putum insaed long dokumen ia mo ol narafala wan we okanaeseisen i divelopem). Mo tu, eksekiutif manejmen i mas sapotem ol IT dipatmen taem oli stap enfosem ol kraeteria long ol disisen blong pem samting. Oli mas dokumentem long wan fomol wei ol disisen blong okanaeseisen blong akseptem ol risk we oli asosiet wetem ol spesifik teknoloji prodak, wan sinia bisnis eksekiutif i mas apruvum, mo presentem long wan rekula wei long Bod blong ol Daerekta.

Ol ki entapraes IT sevis we oli sapotem sikiuriti blong okanaeseisen, olsem entapraes netwok, entapraes aedentiti mo akses manejmen, mo ol sikiuriti opereisen mo ol rispons kapabiliti, oli mas luk olsem ol impoten bisnis fanksen we oli fandem blong alaenem wetem impotens blong sakses blong misen blong okanaeseisen. Ol okanaeseisen oli mas divelopem wan plan blong apgreidem ol kapabiliti ia blong leverejem ol manufakjera we oli holem Sikiua-tru long-Disaen mo Sikiua-tru long-Difolt praktis.

Weaples we i posibol, ol okanaeseisen oli mas trae had blong fojem ol stratejik patna rileisensip wetem ol mein IT saplaea. Ol kaen rileisensip ia oli inkludim trast long maltipol level blong okanaeseisen mo provaedem ol rod blong solvem ol isiu mo aedentifaem ol praeoriti we oli semak bitwin olketa. Sikiuriti i mas wan mein elemen blong ol kaen rileisensip ia mo ol okanaeseisen oli mas trae had blong fosem oltaem impotens blong ol praktis blong Sikiua-tru long-Disaen mo Sikiua-tru long-Difolt long tuketa ol fomol (eksampol ol kontrak o ol venda akrimen) mo ol infomol daemensen blong rileisensip. Ol okanaeseisen oli mas ekspektem transparensi long ol teknoloji saplaea blong olketa abaot ol intenal kontrol standing blong olketa mo tu abaot ol rodmap blong olketa i ko long daereksen blong adoptem ol praktis blong Sikiua-tru long-Disaen mo Sikiua-tru long-Difolt.

Mo tu blong mekem Sikiua-tru long-Difolt wan praeoriti insaed long wan okanaeseisen, ol IT lida oli mas kolaboret wetem ol pia blong olketa insaed long indastri blong andastanem wij prodak mo ol sevis oli bes simbolaesem ol disaen prinsipol ia. Ol lida ia oli mas kodinetem ol rikwes blong olketa blong helpem ol manufakjera oli praeoritaesem ol sikiuriti insietif blong olketa we bae oli hapen long fiuja. Taem oli wok tuketa, ol kastoma oli save helpem blong provaedem miningful input i ko long ol manufakjera mo krietem ol insentif blong olketa blong praeoritaesem sikiuriti.

Taem we ol okanaeseisen oli leverejem ol klaod sistem, oli mas mekem sua se oli andastanem risponsibiliti model we oli serem wetem teknoloji saplaea blong olketa. Hemia hem i minim se, ol okanaeseisen oli mas kat klariti long ol risponsibiliti blong saplaea blong sikiuriti be i no jes risponsibiliti blong kastoma.

Ol okanaeseisen oli mas praeoritaesem ol klaod provaeda we oli transparent abaot sikiuriti standing blong olketa, ol intenal kontrol, mo paoa blong mekem ol oblikeisen blong olketa anda long risponsibiliti model we oli serem.

DISKLEMA

Infomeisen insaed long ripot ia mifala i kivim "olsem we i stap" blong infomeisenal pepes nomo. CISA, mo ol ejensi we oli raetem buk ia oli no endosem eni komesel prodak o sevis, inkludim eni sabjek blong analisis. Eni refrens long ol spesifik komesel entiti o ol komesel prodak, ol proses, o ol sevis tru long sevis mak, tredmak, manufakjera, o hemia we oli no rifea long hem, hem i no minim se CISA mo ol ejensi we oli raetem buk ia oli stap endosem, rekomendem o fevoretem. Dokumen ia hem i wan joen inisietif we CISA i mekem we hem i no otomatikali kam olsem wan rekulatori dokumen.

OL RISOS

CISA

- CISA's SBOM Guidance (SBOM Gaedans blong CISA)
- CISA's Cross-Sector Cybersecurity Performance Goals (Ol Kros-Sekta Pefomens Gol blong CISA)
- Guidelines on Technology Interoperability (Ol Gaedlaen abaot Teknoloji Intaoperabiliti)
- CISA and NIST's Defending Against Software Supply Chain Attacks (Difens blong CISA mo NIST Akensem Ol Sofwea Saplae JenAtak)
- The Cost of Unsafe Technology and What We Can Do About It | CISA (Kost blong Teknoloji we i no Sef mo Wanem Yumi Save Mekem Abaotem)
- Stop Passing the Buck on Cybersecurity: Why Companies Must Build Safety Into Tech Products (foreignaffairs.com) (Stop pasem wok blong Saebasikiuriti: From wanem ol Kampani oli Mas Bildim Sefti i ko Insaed long ol Teknoloji Prodak)
- CISA's Stakeholder-Specific Vulnerability Categorization (SSVC) Guidance (Gaedans blong Stekholda-Spesifik Valnerabiliti Katigoraeseisen blong CISA
- CISA's Phishing Resistant MFA Fact Sheets (Ol MFO Fishing Resisten Fakt Shit)
- Cyber Guidance for Small Businesses | CISA (Saeba Gaedans blong ol Smol Bisnis | CISA)

NSA

- NSA's Cybersecurity Information Sheet on Memory Safety (Saebasikiuriti Infomeisen Shit long Memori Sefti blogn NSA)
- NSA's ESF Securing the Software Supply Chain: Best Practices for Suppliers (ESF blong NSA abaot wok blong sikiurim Sofwea Jein Saplae: Ol Bes Praktis blong ol Saplaea)

FBI

- Understanding and Responding to the SolarWinds Supply Chain Attack: The Federal Perspective (Andastanem mo Ansa long ol SolaWin Saplae Jein Atak: Federel Tingting)
- The Cyber Threat - Response and Reporting (Saeba Tret - Ansa mo Ripot)
- FBI's Cyber Strategy (Saeba Strateji blong FBI)

National Institute of Standards and Technology (NIST)

- NIST's Digital Identity Guidelines (Ol Gaedlaen blong Dijitel Aedentiti blong NIST)
- NIST's Cyber Security Framework (Saeba Sikiuriti Fremwok blong NIST)
- NIST's Secure Software Development Framework (SSDF) (Sikiua Sofwea Divelopmen Fremwok blong NIST)

Saeba Sikiuriti Senta blong Ostrelia (ACSC)

- ACSC's IoT Code of Practice Guidance for Manufacturers (IoT Kod blong Praktis Gaedans we ACSC i mekem blong ol Manufakjera)

The United Kingdom's National Cyber Security Centre (UK)

- The UK's Cyber Assessment Framework (Saeba Asesmen Fremwok blong UK)
- The UK NCSC's Secure Development and Deployment guidance (Sikiua Divelopmen mo Diploemen gaedans blong NCSC blong UK)
- The UK NCSC's Vulnerability Management guidance (Valnerabiliti Manejmen gaedans blong NCSC blong UK)
- The UK NCSC's Vulnerability Disclosure Toolkit (Valnerbiliti Disklosa Tulkit blong NCSC blong UK)

- University of Cambridge's CHERI (CHERI blong Yunivesiti blong Kambrij)
- So long and thanks for all the bits - NCSC.GOV.UK (Long taem mo tankio from evri bit - NCSC.GOV.UK)

Saeba Sikiuriti Senta blong Kanada (CCS)

- CCCS's Guidance on Protecting Against Software Supply Chain Attacks (Gaedans abaot hao blong Protek Akensem ol Sofwea Saplae Jein Atak blong CCCS)
- Cyber supply chain: An approach to assessing risks (Saeba saplae jein: Wan aproj blong asesem ol risk)
- Canadian Centre for Cyber Security's CONTI ransomware guidance (Kanada Senta blong Saeba Sikiuriti blong gaedans blong ransomwea CONTI)

Federel Ofis blong Infomeisen Sikiuriti blong Jemeni (BSI)

- The BSI Grundschutz compendium (module CON.8)
- The international standard IEC 62443, part 4-1 (Intanasonal standed IEC 62443, pat 4-1)
- State of IT-security in Germany report, 2022 (Steit blong IT-sikiuriti long Jenemi ripot, 2022)
- BSI practices of web application security (Ol BSI praktis blong web aplikeisen sikiuriti)

Netherlands' National Cyber Security Centre

- NCSC-NL's Mature Authentication Factsheet (Majua Otentifikeisen Fakt Shit blong NCSC-NL)

Narafala

- How Complex Systems Fail (Olsem wanem Ol Kompleks Sistem Oli Feil)
- The New Look in complex system failure (Niufala luk insaed long kompleks sistem feilia)