TLP:CLEAR

SECURE BY DESIGN

PAGBABAGO SA BALANSE NG PANGANIB SA CYBERSECURITY:

MGA PRINSIPYO AT PAMAMARAAN PARA SA DINISENYONG LIGTAS NA SOFTWARE

TLP:CLEAR

Communications Security Establishment

Canadian Centre for Cyber Security

Centre de la sécurité des télécommunications

Centre canadien pour la cybersécurité

Nilalaman

PANGKALAHATANG IDEYA: HINDI LIGTAS NA DISENYO

Ang teknolohiya ay kasama sa halos lahat ng aspeto ng pang-araw-araw na buhay. Ang mga sistemang nakaharap sa Internet ay konektado sa mga kritikal na sistema na direktang nakakaapekto sa ating pang-ekonomiyang kaunlaran, kabuhayan, at maging sa kalusugan, mula sa pamamahala ng personal na pagkakakilanlan hanggang sa pangangalagang medikal. Ang isang halimbawa ng disbentaha ng naturang mga kaginhawahan ay ang mga pandaigdigang cyber breaches na nagreresulta sa pagkansela ng mga ospital sa mga operasyon at paglilipat ng pangangalaga sa pasyente. Ang hindi ligtas na teknolohiya at mga kahinaan sa mga kritikal na sistema ay maaaring mag-imbita ng mga nakakahamak na pagatake sa cyber, na humahantong sa mga potensyal na panganib sa[1] kaligtasan.

Bilang resulta, napakahalaga para sa mga tagagawa ng software na gawing sentro ang secure by design at secure by default sa disenyo ng produkto at mga proseso ng pagbuo. Ang ilang mga nagbebenta ay gumawa ng mahusay na mga hakbang na nagtutulak sa industriya pasulong sa kasiguruhan ng software, habang ang iba ay nahuhuli. Lubos na hinihikayat ng mga ahensyang may-akda sa bawat tagagawa ng teknolohiya na gagawin ang kanilang mga produkto sa paraang binabawasan ang pasanin ng mga mamimili ang patuloy na pagsasagawa ng pagsubaybay, mga regular na pag-update, at kontrol sa pagkapinsala sa kanilang mga sistema upang mabawasan ang mga paghihimasok ng cyber. Hinihimok din namin ang mga tagagawa ng software na buuin ang kanilang mga produkto sa paraang nagpapadali sa pagiging awtomatiko ang pagsasaayos, pagsubaybay, at mga regular na update. Hinihikayat ang mga tagagawa na akuin ang pagpapahusay ng mga resulta ng seguridad ng kanilang mga mamimili. Dati nang umaasa ang mga tagagawa ng teknolohiya sa pag-aayos ng mga kahinaan na natagpuan pagkatapos na ipadala ng mga mamimili ang mga produkto, at ang mga mamimili ang kailangang maglapat sa mga patch sa kanilang sariling gastos. Sa pamamagitan lamang ng pagsasama ng mga kasanayan sa secure-by-design na mahihinto natin ang paulit-ulit na paglikha at paglalapat ng mga solusyon. **Tala:** Ang terminong "secure by design" ay sumasaklaw sa parehong secure by design at secure by default.

Upang maisakatuparan ang mataas na pamantayang ito ng seguridad ng software, hinihikayat ng mga ahensyang may-akda ang mga tagagawa na unahin ang integrasyon ng seguridad ng produkto bilang isang kritikal na pangangailangang aspeto at paglabas nito sa merkado. Unti-unti, makakagawa ang mga engineering team ng isang bagong steady-state na ritmo kung saan ang seguridad ay isinama sa disenyo at nangangailangan ng kaunting trabaho lamang upang mapanatili ito.

Katulad sa pananaw na ito, pinatitibay ng European Union ang kahalagahan ng seguridad ng produkto sa Cyber-Resilience-Act, na binibigyang-diin na dapat ipatupad ng mga tagagawa ang seguridad sa buong siklo ng buhay ng isang produkto upang maiwasan ng mga tagagawa na magpapasok ng mga hindi ligtas na produkto sa merkado.

[1] Kinikilala ng mga samahang may-akda na ang terminong "kaligtasan" ay may maraming kahulugan depende sa kontekstong ginamit nito. Para sa mga layunin ng gabay na ito, ang "kaligtasan" ay tumutukoy sa pagtataas ng mga pamantayan sa seguridad ng teknolohiya upang maprotektahan ang mga mamimili mula sa malisyosong aktibidad sa cyber.

Upang lumikha ng kinabukasan kung saan ang teknolohiya at mga nauugnay na produkto ay mas ligtas para sa mga mamimili, hinihimok ng mga samahang may-akda ang mga tagagawa na baguhin ang kanilang mga programa sa disenyo at pagpapaunlad upang payagan lamang ang mga secure-by-design at default na mga produkto na maipadala sa mga mamimili. Bago pa ang paggawa, ang mga produktong secure by design ay nakonsepto kung saan ang seguridad ng mga mamimili ang pangunahing layunin sa negosyo, hindi lamang isang teknikal na katangian. Ang mga produktong secure-by-design ay nagsisimula sa layuning iyon bago pa man simulan ang paggawa. Ang mga kasalukuyang produkto ay maaaring magingisang secure by design na estado sa maraming mga pag-ulit. Ang mga secure by default na mga produkto ay ang mga ligtas na gamitin “out of the box” na may kaunti o walang kinakailangang pagbabago sa pagsasaayos, at may mga katangian ng seguridad nang walang karagdagang gastos. Inililipat ng dalawang prinsipyong ito sa mga tagagawa ang karamihan sa malaking pasanin sa pagpapanatiling ligtas ang produkto, at binabawasan ang mga pagkakataong mabiktima ang mga mamimili ng mga insidente sa seguridad na nagreresulta mula sa mga maling pagsasaayos, hindi sapat na mabilis na pag-patch, o marami pang karaniwang isyu.

Ang Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA), Federal Bureau of Investigation (FBI) at ang mga sumusunod na internasyonal na partners[2] ay nagbibigay ng mga rekomendasyon sa gabay na ito bilang isang roadmap para sa mga tagagawa ng software upang matiyak ang seguridad ng kanilang mga produkto:

- Sentro ng Cyber Security ng Australia (ACSC)
- Sentro ng Cyber Security ng Canada (CCCS)
- Pambansang Sentro ng Cyber Security ng United Kingdom (NCSC-UK)
- Tanggapang pang Pederal para sa Seguridad ng Impormasyon ng Germany (BSI)
- Pambansang Sentro ng Cyber Security ng Netherlands (NCSC-NL)
- Pambansang Sentro ng Cyber Security ng Norway (NCSC-NO)
- Computer Emergency Response Team New Zealand (CERT NZ) at Pambansang Sentro ng Cyber Security ng New Zealand (NCSC-NZ).
- Ahensya ng Internet at Seguridad ng Korea (KISA)
- Pambansang Cyber Directorate ng Israel (INCD)
- Pambansang Sentro ng Incident Readiness at Stratehiya para sa Cybersecurity ng Japan (NISC) at ang Computer Emergency Response Team Coordination Center ng Japan (JPCERT/CC)
- OAS/CICTE Network ng Cyber Incident Response Teams (CSIRT) ng Gobyerno ng Americas
- Ahensya ng Cyber Security ng Singapore (CSA)
- Pambansang Ahensya ng Seguridad sa Cyber at Impormasyon ng Czech Republic (NÚKIB)

Kinikilala ng mga ahensyang may-akda ang mga kontribusyon ng maraming kasosyo sa pribadong sektor sa pagsulong ng security-by-design at security-by-default. Nilalayon ng produktong ito na isulong ang isang pang-internasyonal na pag-uusap tungkol sa mga pangunahing priyoridad, pamumuhunan, at pagpapasya na kinakailangan para makamit ang hinaharap kung saan ligtas, mapagkakatiwalaan, at matibay ang teknolohiya sa pamamagitan ng disenyo at default. Para sa layuning iyon, ang mga samahang may-akda ay humihingi ng tugon sa produktong ito mula sa mga interesadong partido at nilalayon na magpulong ng isang serye ng mga sesyon ng pakikinig upang higit na pinuhin, tukuyin, at isulong ang aming gabay upang makamit ang aming mga ibinahaging layunin.

Para sa karagdagang impormasyon sa kahalagahan ng kaligtasan ng produkto, tingnan ang artikulo ng CISA, Ang Halaga ng Hindi Ligtas na Teknolohiya at Ano ang Magagawa Natin Tungkol Dito (The Cost of Unsafe Technology and What We Can Do About It)

[2] Mula dito ay tinukoy bilang ang "mga samahang may-akda."

ANO ANG BAGO

Ang paunang paglalathala ng ulat na ito ay nakabuo ng maraming mahalagang mga pag-uusap sa loob ng industriya ng software. Ang pang-araw-araw na balita ng mga organisasyon at indibidwal na nakompromiso ay nagpapakita ng pangangailangan para sa higit pang pag-uusap tungkol sa kung paano matugunan ang mga talamak at sistematikong problema sa mga produkto ng software.

Pagkatapos ng paglabas noong Abril 2023, ang mga ahensyang may-akda (mula ngayon ay tinutukoy bilang "kami" at "amin") ay nakatanggap ng maingat na pagpuna mula sa daan-daang indibidwal, kumpanya, at mga asosasyon sa kalakalan. Ang pinakakaraniwang kahilingan sa pagpuna ay ang magbigay ng higit pang detalye sa tatlong prinsipyo habang nalalapat ang mga ito sa parehong mga tagagawa ng software at sa kanilang mga mamimili. Sa dokumentong ito, pinalawak namin ang orihinal na ulat at isinali namin ang iba pang mga tema gaya ng laki ng tagagawa at mamimili, maturity ng mamimili, at ang saklaw ng mga prinsipyo.

Ang software ay nasa lahat ng dako at walang iisang ulat ang makakasaklaw nang sapat sa buong hanay ng mga sistema ng software, pagbuo ng mga produkto ng software, pag-deploy at pagmementena ng mamimili, at pagsasama sa iba pang mga sistema. Para sa gabay sa ibaba na hindi malinaw na nagmamapa sa isang partikular na kapaligiran, inaasahan naming marinig mula sa komunidad kung paano nakatulong ang mga kasanayang inilarawan sa papel na ito sa mga partikular na pagpapabuti sa seguridad.

Nalalapat din ang ulat na ito sa mga tagagawa ng mga sistema at modelo ng software ng artificial intelligence (AI). Bagama't maaaring iba ang mga ito sa mga tradisyonal na anyo ng software, nalalapat pa rin ang mga pangunahing kasanayan sa seguridad sa mga sistema at modelo ng AI. Maaaring mangailangan ng pagbabago ang ilang secure by design na kasanayan upang maisaalang-alang ang mga partikular na pagsasaalang-alang sa AI, ngunit ang tatlong pangkalahatang secure by design na mga prinsipyo ay nalalapat sa lahat ng sistema ng AI.

Kinikilala namin na ang pagbabago ng isang software development lifecycle (SDLC) upang iayon sa mga prinsipyo ng secure by design ay hindi isang simpleng gawain at maaaring matagal gawin. Dagdag pa, maaaring mahirapan ang mga mas maliliit na tagagawa ng software na ipatupad ang marami sa mga mungkahing ito. Naniniwala kami na kailangan ng industriya ng software na gawing malawakang magamit ang mga kagamitan at pamamaraan na ginagawang mas ligtas ang mga produkto. Habang mas maraming tao at organisasyon ang tumutuon sa kanilang atensyon sa mga pagpapahusay sa seguridad ng software, naniniwala kaming may puwang para sa mga inobasyon na magpapaliit sa agwat sa pagitan ng mas malaki at mas maliliit na tagagawa ng software para sa kapakinabangan ng lahat ng mamimili.

Ang update na ito sa orihinal na secure by design na ulat ay bahagi ng aming pangako na bumuo ng mga partnership sa maraming magkakaugnay na komunidad ng stakeholder na sumusuporta sa aming teknolohikal na ecosystem. Ito ay resulta ng tugon mula sa maraming bahagi ng ecosystem na iyon, at patuloy kaming makikinig at matututo mula sa mga pananaw. Bagama't maraming mga hamon sa hinaharap, umaasa pa rin kami habang naririnig namin ang kadalasang matagumpay na kwento ng mga tao at organisasyon na gumagamit ng secure by design na pilosopiya.

PAANO GAMITIN ANG DOKUMENTO

Hinihikayat namin ang mga tagagawa ng software na sumunod sa mga prinsipyo sa loob ng dokumentong ito. Maaaring ipakita ng mga tagagawa ng software ang kanilang pangako sa pamamagitan ng pampublikong pagdodokumento ng kanilang mga aksyong ginawa, alinsunod sa mga hakbang na nakalista sa ibaba. Hinihikayat namin ang mga tagagawa ng software na maghanap ng mga taktika na tumutugon sa diwa ng prinsipyong ito at lumikha ng mga artifact na bubuo ng isang nakakahimok na kaso na kahit ang nag-aalinlangan na kasalukuyan at potensyal na mga mamimili na kanilang kinakatawan ang secure by design na pilosopiya.

Bilang karagdagan sa mga aksyon na dapat gawin ng mga tagagawa ng software, maaari ding gamitin ng mga mamimili ang dokumentong ito. Ang mga kumpanyang bumibili ng software ay dapat magtanong ng mahihirap na tanong sa kanilang mga vendor, na kumukuha ng inspirasyon mula sa mga halimbawa ng pagsunod sa mga prinsipyong nakalista sa dokumentong ito. Sa paggawa nito, makakatulong ang mga mamimili na ilipat ang merkado patungo sa mga produktong mas ligtas sa pamamagitan ng disenyo. Ang isang halimbawa ng mga tanong na maaaring itanong ng mga mamimili sa mga vendor ay ibinibigay sa Gabay para sa K-12 Technology Acquisitions ng CISA.

Hinihikayat namin ang mga mamimili sa negosyo na isama ang mga kasanayang ito sa mga proseso ng pagkuha, mga pagtatasa ng angkop na pagsusumikap ng vendor, mga desisyon sa pagtanggap sa panganib ng enterprise, at iba pang hakbang na ginawa kapag sinusuri ang mga vendor. Dapat ding itulak ng mga mamimili ang kanilang mga vendor na idokumento sa publiko ang secure by design na mga aksyon na ginagawa ng bawat vendor. Sama-sama, maaari itong lumikha ng isang malakas na senyas ng demanda para sa seguridad, na maaaring maghikayat at magbigay daan sa mga tagagawa ng software na gumawa ng mga hakbang tungo sa higit na seguridad. Sa madaling salita, kung paanong hinahangad nating lumikha ng malawakang pilosopiya ng secure by design sa loob ng mga tagagawa ng software, kailangan nating lumikha ng kulturang "secure by demand" sa kanilang mga mamimili.

Secure by Design

Ang ibig sabihin ng “secure by design” ay ang mga produkto ng teknolohiya ay binuo sa paraang makatuwirang nagpoprotekta laban sa mga nakakahamak na cyber actor na matagumpay na nakakuha ng access sa mga aparato, datos, at konektadong imprastraktura. Ang mga tagagawa ng software ay dapat magsagawa ng pagtatasa ng panganib upang matukoy at mabilang ang laganap na mga banta sa cyber sa mga kritikal na sistema, at pagkatapos ay isama ang mga proteksyon sa mga blueprint ng produkto na tumutukoy sa umuusbong na tanawin ng pagbabanta sa cyber.

Inirerekomenda din ang mga kasanayan sa paggawa ng ligtas na information technology (IT) at maraming layer ng depensa—na kilala bilang defense-in-depth—para pigilan ang mga malisyosong aktor na maikompromiso ang mga sistema o makakuha ng hindi awtorisadong pag-access sa sensitibong datos. Ang mga ahensyang may-akda ay higit pang nagrerekomenda sa mga tagagawa na gumamit ng isang iniangkop na modelo ng pagbabanta sa panahon ng pagbuo ng produkto upang matugunan ang lahat ng mga potensyal na banta sa isang sistema at isaalang-alang ang proseso ng paggamit ng bawat sistema.

Hinihimok ng mga organisasyong may-akda ang mga tagagawa na kumuha ng panlahatang pamaraan sa seguridad para sa kanilang mga produkto at plataporma. Nangangailangan sa paggawa ng secure by design ang istratehikong pamumuhunan ng mga nakalaang mapagkukunan ng mga tagagawa ng software sa bawat sapin ng disenyo ng produkto at proseso ng paggawa na hindi maaaring "bolted on" sa ibang pagkakataon. Nangangailangan ito ng matibay na pamumuno ng mga nangungunang executive ng negosyo ng tagagawa para gawing priyoridad sa negosyo ang seguridad, hindi isang teknikal na katangian lang. Ang pakikipagtulungang ito sa pagitan ng mga pinuno ng negosyo at mga teknikal na koponan ay umaabot mula sa mga paunang yugto ng disenyo at paggawa, sa pamamagitan ng pag-deploy at pagmementena ng mamimili. Hinihikayat ang mga tagagawa na gumawa ng mahirap na mga pagpapalitan (trade-off) at pamumuhunan, kabilang ang mga "hindi nakikita" ng mga mamimili (hal., paglipat sa mga programming language na nag-aalis ng mga malawakang kahinaan). Dapat nilang unahin ang mga katangian, mekanismo, at pagpapatupad ng mga gamit na nagpoprotekta sa mga mamimili kaysa sa mga katangian ng produkto na mukhang kaakit-akit ngunit nagpapalaki sa attack surface.

Walang isang solusyon upang wakasan ang patuloy na banta ng mga malisyosong cyber actor na nagsasamantala sa mga kahinaan sa teknolohiya, at ang mga produkto na "secure by design" ay patuloy na magdaranas ng mga kahinaan; gayunpaman, ang isang malaking hanay ng mga kahinaan ay dahil sa isang medyo maliit na subset ng mga sanhing ugat. Ang mga tagagawa ay dapat bumuo ng mga nakasulat na roadmap upang ihanay ang kanilang mga kasalukuyang portfolio (karpeta) ng produkto sa mas secure by design na kasanayan, na tinitiyak na lumilihis lamang sa mga pambihirang sitwasyon.

Kinikilala ng mga organisasyong may-akda na ang pagtanggap sa responsibilidad sa mga resulta ng seguridad para sa mga mamimili at pagtiyak sa antas ng seguridad ng mamimili na ito ay maaaring magpataas ng mga gastos sa pagpapaunlad. Gayunpaman, ang pamumuhunan sa secure by design na mga kasanayan habang gumagawa ng mga makabagong produkto ng teknolohiya at pagmementena sa mga umiiral na ay maaaring makabuluhang mapabuti sa postura ng seguridad ng mga mamimili at mabawasan ang posibilidad ng kompromiso. Ang mga prinsipyo ng secure by design ay hindi lamang nagpapatibay sa postura ng seguridad para sa mga mamimili at reputasyon ng brand para sa mga tagagawa ngunit ang kasanayan ay nagpapababa rin sa mga gastos sa pagpapanatili at pag-patch para sa mga tagagawa sa mahabang panahon.

Ang seksyong Mga Rekomendasyon para sa Mga Tagagawa ng Software na nakalista sa ibaba ay nagbibigay ng listahan ng mga kasanayan at patakaran sa pagbuo ng produkto para isaalang-alang ng mga tagagawa.

Secure by Default

Ang ibig sabihin ng "secure-by-default" ay ang mga produkto ay handa laban sa laganap na mga pamaraang "out of the box" nang walang karagdagang bayad. Ang mga produktong ito ay nagpoprotekta laban sa pinakalaganap na mga banta at kahinaan at hindi kinakailangang gumawa ng karagdagang mga hakbang ang mga end-user upang mapatibay ang mga ito. Ang mga produkto na secure-by-default ay idinisenyo upang ipaalam sa mga mamimili na kapag lumihis sila mula sa mga ligtas na default, pinapataas nila ang posibilidad na makompromiso maliban kung magpapatupad sila ng mga karagdagang kontrol para matumbasan ito. Ang secure by default ay isang paraan ng secure by design.

- Ang ligtas na pagsasaayos ay dapat ang default na baseline. Awtomatikong pinapagana ng mga secure-by-default na mga produkto ang pinakamahalagang kontrol sa seguridad na kailangan upang maprotektahan ang mga negosyo mula sa mga malisyosong cyber actor, at magbigay ng kakayahang magamit at makonpigura ang mga kontrol sa seguridad nang walang karagdagang gastos.
- Ang pagiging kumplikado ng pagsasaayaos ng seguridad ay hindi dapat maging problema ng mamimili. Ang mga kawani ng organisasyong IT ay madalas na napupuno ng mga responsibilidad sa seguridad at pagpapatakbo, kaya nagreresulta sa limitadong oras upang maunawaan at maipatupad ang mga implikasyon sa seguridad at pagpapagaan na kinakailangan para sa isang matatag na kaayusan ng cybersecurity. Sa pamamagitan ng lubusang paggamit ng matatag na paghubog ng produkto—pagpapatatag sa "default path"—matutulungan ng mga tagagawa ang kanilang mga mamimili sa pamamagitan ng pagtiyak na ang kanilang mga produkto ay ginawa, ipinamamahagi, at ginagamit nang matatag alinsunod sa mga pamantayang "secure-by-default".

Ang mga tagagawa ng mga produkto na "secure-by-default" ay hindi naniningil ng dagdag para sa pagpapatupad ng mga karagdagang konpigurasyon ng seguridad. Sa halip, isinama nila ang mga ito sa pangunahing produkto, kagaya ng mga seatbelt na kasama sa lahat ng bagong kotse.

Ang seguridad ay hindi isang marangyang opsyon, kung hindi isang pamantayan na dapat asahan ng bawat mamimili nang hindi nakikipag-areglo o nagbabayad ng higit pa.

MGA REKOMENDASYON PARA SA MGA TAGAGAWA NG SOFTWARE

Ang pinagsamang gabay na ito ay nagbibigay ng mga rekomendasyon sa mga tagagawa para sa pagbuo ng isang nakasulat na roadmap (plano) upang maipatupad at matiyak ang seguridad ng IT. Inirerekomenda ng mga may-akdang ahensya sa mga tagagawa ng software na ipatupad ang mga stratehiya na nakabalangkas sa mga seksyon sa ibaba upang akuin ang mga resulta ng seguridad ng kanilang mga mamimili sa pamamagitan ng mga prinsipyong secure-by-design at -default.

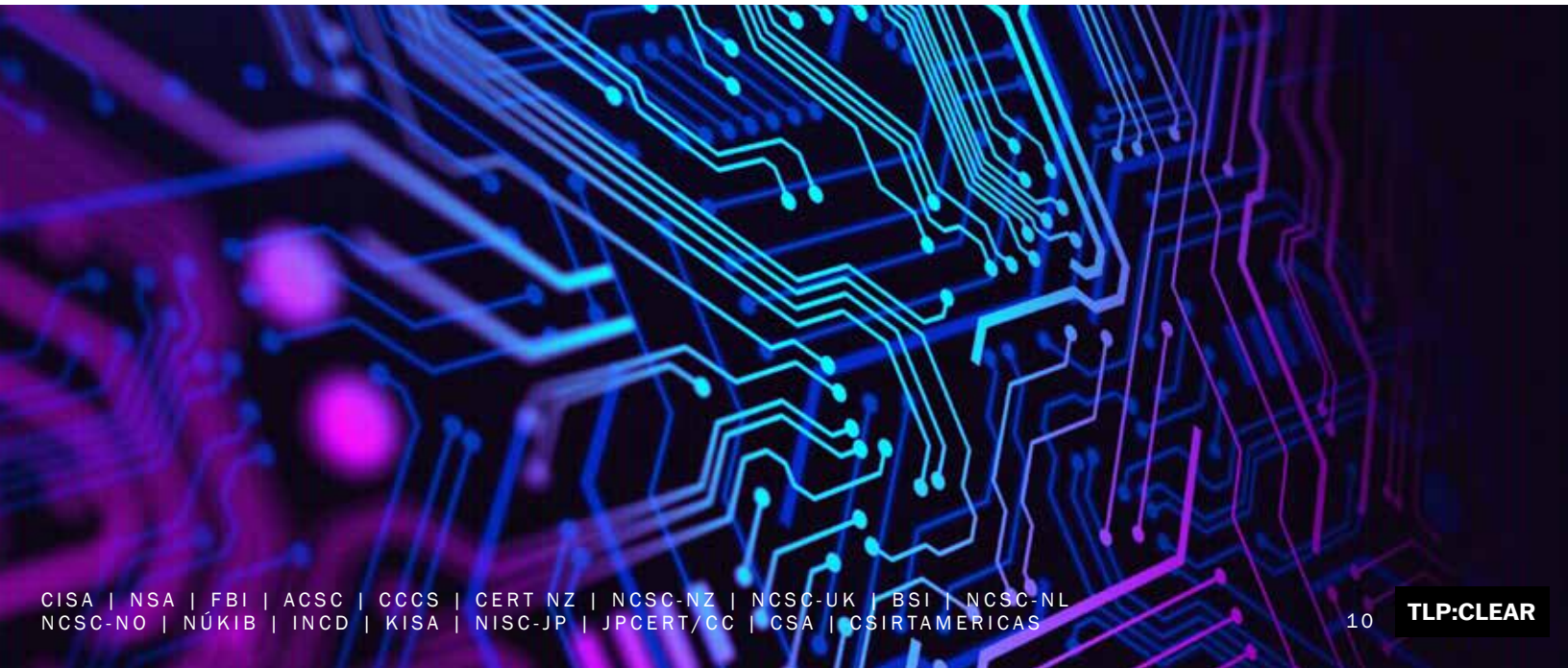
MGA PRINSIPYO SA SEGURIDAD NG PRODUKTONG SOFTWARE

Hinihikayat ang mga tagagawa ng teknolohiya na magpatupad ng istratehiya na nagbibigay-priyoridad sa seguridad ng software. Binuo ng mga ahensyang may-akda ang tatlong pangunahing prinsipyo sa ibaba upang gabayan ang mga tagagawa ng software sa pagbuo ng seguridad ng software sa kanilang mga proseso ng disenyo bago gagawin, isaayos, at ipadala ang kanilang mga produkto.

1 **Tanggapin ang responsibilidad ng mga resulta ng seguridad ng mamimili** at baguhin ang mga produkto nang naaayon. Ang pasanin ng seguridad ay hindi dapat ipasa lamang sa mamimili.

2 **Tanggapin ang radikal na katapatan at pananagutan.**
Dapat ipagmalaki ng mga tagagawa ng software ang kanilang sarili sa paghahatid ng mga ligtas at matatag na produkto, pati na rin ang pagkakaiba ng kanilang sarili sa ibang mga tagagawa batay sa kanilang kakayahang gawin ito. Maaaring kabilang dito ang pagbabahagi ng impormasyong natutunan nila mula sa kanilang mga deployment sa mamimili, gaya ng paggamit ng malakas na mekanismo ng pagpapatunay bilang default. Kasama rin dito ang pangakong titiyaking kumpleto at tumpak ang mga pagpapayo sa kahinaan at nauugnay na mga talaan ng mga karaniwang kahinaan at pagkalantad (CVE). Gayunpaman, mag-ingat na hindi palaging bilangin ang mga CVE bilang negatibong panukat, dahil ang mga bilang na ito ay tanda rin ng isang malusog na komunidad ng pagtatasa sa kodigo at pagsusuri.

3 **Lumikha ng istruktura at pamumuno ng organisasyon upang makamit ang mga layuning ito.**
Habang ang kadalubhasaan sa teknikal na paksa ay kritikal sa seguridad ng produkto, ang mga senior executive ang pangunahing gumagawa ng desisyon para sa pagpapatupad ng pagbabago sa isang organisasyon. Kailangang unahin ng mga executive ang seguridad bilang isang kritikal na bahagi sa pagbuo ng produkto sa buong organisasyon, at sa pakikipagtulungan ng mga mamimili.



Upang masunod ang tatlong prinsipyong ito, dapat isaalang-alang ng mga tagagawa ang ilang mga taktika sa pagpapatakbo upang mabago ang kanilang mga proseso sa paglikha.

Magsagawa ng mga regular na pagpupulong kasama ang pamunuang ehekotibo ng kumpanya upang himukin ang kahalagahan ng secure-by-design at secure-by-default sa loob ng organisasyon. Dapat na maitatag ang mga patakaran at pamamaraan para gantimpalaan ang mga pangkat sa paggawa na lumikha sa mga produkto na sumusunod sa mga prinsipyong ito, kagaya ng mga parangal para sa pagpapatupad ng mga namumukod-tanging kasanayan sa seguridad ng software o mga insentibo at kriteria para sa pag-akyat at promosyon sa trabaho.

Bigyang kahalagahan ang seguridad ng software sa tagumpay ng negosyo. Halimbawa, isaalang-alang ang pagtalaga ng isang "software security leader" o isang "software security team" na sumusuporta sa mga kasanayan sa negosyo at IT upang direktang mai-ugnay ang mga pamantayan sa seguridad ng software at pananagutan ng gumagawa. Dapat tiyakin ng mga tagagawa na mayroon silang matatag, independiyenteng pagtatasa sa seguridad ng produkto at mga programa sa pagsusuri para sa kanilang mga produkto.

Gumamit ng isang iniangkop na modelo ng pagbabanta sa panahon ng paglalaan at pag-unlad ng mapagkukunan upang bigyang-priyoridad ang mga pinaka-kritikal at may mataas na epekto na mga katangian. Isinasaalang-alang ng mga modelo ng pagbabanta ang partikular na use-case ng isang produkto at binibigyang-daan ang mga pangkat sa paglikha na palakasin ang mga produkto. Panghuli, dapat na papanagutin ng senior leadership ang mga pangkat sa paghahatid ng mga ligtas na produkto bilang pangunahing elemento ng kahusayan at kalidad ng produkto.

Bilang bahagi ng Oktubre 2023 update sa gabay na ito, ang tatlong prinsipyong ito ay pinalawak sa pamamagitan ng mga sumusunod na paliwanag, pagpapakita, at ebidensya.

PRINSIPYO 1: Tanggapin ang Responsibilidad sa mga Resulta sa Seguridad ng Mamimili

PAGPAPALIWANAG

Idinidikta ng mga modernong pinakamahusay na kagawian na mamumuhunan ang mga tagagawa ng software sa mga pagsusumikap sa seguridad ng produkto na kinabibilangan ng **pagpapatigas ng aplikasyon, mga katangian ng aplikasyon,** at **default setting ng aplikasyon.**

Kailangan ng mga tagagawa ng software na ipatupad ang **application hardening** sa pamamagitan ng paggamit ng mga proseso at teknolohiya na nagpapataas ng gastos para sa isang malisyosong aktor na gustong ikompromiso ang mga aplikasyon. Ang mga protocol at pamamaraan ng pagpapatigas ng aplikasyon ay tumutulong sa mga produkto na labanan ang mga pag-atake ng mga matatalinong malisyosong aktor. Ang mga tuntunin katulad ng hardening, seguridad ng produkto, at katatagan ay malapit na nauugnay sa kalidad ng produkto. Ang ideya ay ang seguridad ay dapat na "naka-baked in," at hindi "naka-bolted on." [1] Sa pamamagitan ng pagsaklaw sa seguridad, hindi lamang mapapalaki ng mga tagagawa ng software ang seguridad ng kanilang mga mamimili ngunit mapapataas din ang kalidad ng kanilang mga produkto. Kasama sa mga halimbawang taktika ang pagtiyak na ang input ng gumagamit ay napatunayan at nalinisan, at hindi direktang inilalagay sa code (ibig sabihin, sa pamamagitan ng paggamit ng mga parameterized na query), paggamit ang isang memory safe programming language, mahigpit na pamamahala ng software development life cycle (SDLC), at paggamit ng hardware-backed cryptographic key na pamamahala.

Kailangang suportahan ng mga aplikasyon ang **mga katangian ng aplikasyon** na nauugnay sa cybersecurity. Kung minsan ay tinatawag na "mga kakayahan," ang mga katangian na ito ay nagpapalawak ng functionality ng isang produkto o serbisyo sa mga paraan na makakatulong na mapanatili o mapataas ang tindig ng seguridad ng isang mamimili.

Kabilang sa mga halimbawang katangian na nauugnay sa seguridad ang pagsuporta sa transport layer security (TLS) para sa lahat ng koneksyon sa network, single sign on (SSO) support, multi-factor authentication (MFA) support, security event audit logging, role-based access control (RBAC), at attribute-based access control (ABAC).

Nahuhubog ang ilan sa mga katangian ng produkto na ito kaya nagbibigay-daan sa mga mamimili na mas madaling isama ang produkto sa kanilang mga kasalukuyang kapaligiran at daloy ng trabaho. Nangangahulugan na ang mga pagsasaayos na iyon sa mga application ay dapat na may **mga default na setting** hanggang sa isaayos ng mga mamimili ang mga ito. Ang mga default na setting na iyon ay kailangang itakda nang ligtas "out of the box" para ang mga mamimili ay gumamit ng mas kaunting mga mapagkukunan upang gawing mas ligtas ang kanilang mga produkto ng teknolohiya.

Ang bawat isa sa mga elementong ito - pagpapatigas ng aplikasyon, mga tampok ng seguridad ng aplikasyon, at mga default na setting ng aplikasyon - ay gumaganap ng isang papel sa seguridad ng aplikasyon, at ang nagresultang tindig ng seguridad ng mamimili. Dapat isipin ng mga tagagawa ng software ang bawat isa sa mga elementong ito at kung paano nauugnay ang mga ito sa isa't isa. Dapat isipin ng mga tagagawa ang higit pa sa kanilang mga pamumuhunan upang maisama ang mga elementong ito sa kanilang mga produkto. Dapat itong gawin ng mga tagagawa nang higit pa at isaalang-alang kung paano binabago ng mga elementong iyon ang tunay na tindig ng seguridad ng kanilang mga mamimili, para sa mas mabuti o mas masahol pa.

Dapat tanggapin na responsibilidad ng mga tagagawa ang mga resulta ng seguridad ng kanilang mga mamimili sa halip na sukatin ang kanilang sarili sa kanilang mga pagsisikap at pamumuhunan. Ang responsibilidad ay dapat ilagay sa mga tagagawa, kung saan ito ay may pinakamalaking posibilidad na mabawasan ang mga pagkakataon ng kompromiso.

Sa kasamaang palad, hindi ito ang kaso ngayon. Masyadong maraming tagagawa ang naglalagay ng pasan ng seguridad sa mamimili sa halip na mamuhunan sa komprehensibong **application hardening.** Halimbawa, kapag ang tagagawa ay nag-patch ng isang kahinaan, madalas naming nakikita ang mga katulad na kahinaan na nakalantad dahil tinugunan nila ang sintomas sa halip na ang pangunahing sanhi ng depektong iyon. Maaaring magpatupad ang produkto ng iba't ibang pagpapagaan sa iba't ibang bahagi ng code base para sa parehong klase ng kahinaan. Bilang halimbawa, pagkatapos ayusin ng tagagawa ang isang kahinaan sa input sanitization, nakahanap ang mga mananaliksik o ang mga umaatake ng mga code path na hindi nakinabang sa pinahusay na input sanitization. Ang inilapat ng tagagawa ay nag-aayos nang paisa-isa sa halip na pag-isahin ang codebase upang alisin ang klase ng kahinaan sa buong application.

Mga katangian ng application ay maaaring lumikha ng parehong mga benepisyo at panganib para sa mga mamimili. Ang mga katangian na nagbibigay-daan sa mga integration point sa maraming panlabas na sistema at bersyon ay maaaring lubos na magpapataas sa halaga ng isang produkto. Gayunpaman, ang pagsuporta sa mga katangian na walang plano sa pagreretiro, tulad ng isang networking protocol, ay maaaring maglagay sa peligro sa mga mamimili na kulang ang pang-unawa sa mga epekto ng patuloy na paggamit ng katangiang iyon. Halimbawa, ang ilang produkto ay patuloy na gumagamit ng mga networking protocol na nagmula noong 1990s o 2000s at ngayon ay kilala bilang hindi ligtas. Maraming mga dahilan na maaaring makapagpabagal sa bilis ng papapahusay at pagkakalagay ng mga modernong hakbang sa seguridad ng mga mamimili. Maaari silang gumamit ng mga produkto na sumasama sa iba pang network ng organisasyon, ngunit walang mga modernong hakbang sa seguridad, na pumipigil sa IT team sa pagmomoderno. Gayunpaman, maaaring isali ng mga tagagawa ng software ang mga padron na ito sa kanilang proseso ng pagpaplano upang hikayatin ang mga mamimili na manatiling napapanahon.

Mga default na setting ng application ay isang karagdagang lugar ng potensyal na panganib para sa mga mamimili. Kadalasang pinipili ng mga tagagawa ang ilang mga default setting, na ginagawang mas madali para sa mga mamimili na gamitin ang mga katangian ng application na gusto nila. Ang depekto ay pinapataas ng kasanayang ito ang attack surface para sa mga mamimili na maaaring hindi nangangailangan ng ilang katangian at protocol na nakalagay bilang default. Dagdag pa dito, maraming mga kontrol sa seguridad ang naka-off bilang default o nangangailangan ng mga mamimili na maglaan ng oras upang isaayos ang kanilang mga setting upang mapataas ang seguridad. Ang tahasang pagmomodelo ng pagbabanta ay isang taktika na maaaring makatulong sa pagpapasya kung aling mga katangian ang dapat na naka-on bilang default o kung aling mga setting ang kailangan upang maging secure by default. Ang isa pang taktika ay ang magsiyasat ng mga paraan upang mas madaling matutuklasan ang mga katangian para sa administrator.

Ang ilang mga tagagawa ay nagpapadala ng mga produkto na may mga default na maaaring lumikha ng panganib para sa ilan o lahat ng kanilang mga mamimili. Sa halip na magtakda ng mas ligtas na mga default, madalas nilang pinipiling gumawa ng **gabay sa pagpapatigas** na dapat ipatupad ng mga mamimili sa sarili nilang gastos. Ang mga gabay sa pagpapatigas ay dumaranas ng ilang karaniwang problema. Ang ilang gabay sa pagpapatigas ay mahirap hanapin at hindi suportado ng mabuti. Ang iba ay mahirap ipatupad, paminsan-minsan ay nangangailangan ng pagbuo ng software upang magsulat ng isang extension module. Gayunpaman, ipinapalagay ng iba na ang mambabasa ay may malawak na karanasan sa cybersecurity upang maunawaan ang mga paraan kung saan binabago ng iba't ibang mga setting ang attack surface. Ang mga practitioner na may hindi kumpletong pag-unawa sa mga paraan ng mga umaatake ay maaaring mabigo sa wastong pagpapatupad ng mga tagubilin sa gabay ng pagpapatigas, lalo na kung ang mga tagubilin ay hindi ginagawang malinaw ang mga trade off. Dagdag pa, hindi lahat ng gabay sa pagpapatigas ay isinulat ng mga inhinyero na pamilyar sa mga taktika at ekonomiya ng attacker, na nagiging dahilan upang lumikha sila ng mga hardening guide na hindi epektibo kahit na matapat na ipinatupad. Milyun-milyong mamimili ang umaako sa responsibilidad na patigasin ang maraming pagkakataon ng software o mga sistema, kadalasan sa mga kapaligirang limitado ang mapagkukunan. Ang pag-asa sa mga gabay sa hardening ay hindi sapat.

Dapat na patuloy na suriin ang mga setting ng application kung ang mga setting ay ang default o itinakda ng mamimili, laban sa kasalukuyang pag-unawa ng tagagawa sa kalawakan ng pagbabanta. Ang mga aplikasyon ay dapat gawin na may malinaw na mga tagapagpahiwatig tungkol sa mga potensyal na panganib na maaaring magresulta mula sa mga setting na iyon at dapat ipaalam ang mga tagapagpahiwatig na iyon. Tulad ng isang modernong kotse na may indicator tungkol sa mga seatbelt at nagpapahayag ng indicator na iyon sa pamamagitan ng pagpapatunog ng isang alerto kung susubukan mong magmaneho nang hindi nakalagay ang seatbelt, ang software ay dapat magpahayag ng mga palatandaan tungkol sa estado ng seguridad ng isang sistema. Kung ang isang aplikasyon ay naisaayos na hindi nangangailangan ng MFA para sa mga kuwenta ng administrador, dapat nitong ipaalam nang regular sa mga administrator na sila at ang kanilang buong organisasyon ay nasa panganib kung hindi nila isaayos ang MFA. Bukod pa rito, kung ang isang application ay naisaayos upang suportahan ang mga mas lumang protocol na ngayon ay kilala na nagpapatupad ng mahinang cryptography, dapat itong regular na gawing malinaw sa mga administrador na ang organisasyon ay nasa panganib at magbigay ng mga mapagkukunan upang malutas ang sitwasyon. Hinihimok namin ang mga tagagawa na ipatupad ang mga nakagawiang nudge na nakapaloob sa produkto sa halip na umasa sa mga administrador na magkaroon ng oras, kadalubhasaan, at kamalayan upang bigyang-kahulugan ang mga gabay sa pagpapatigas. Malinaw na umiiral ang mga pagkakataon para sa pagbabago upang balansehin ang mga pagsasaalang-alang sa seguridad at kakayahang magamit.

Ang bawat isa sa mga elemento sa itaas ay lumilikha ng isang hindi maaasahan na sitwasyon kung saan ang mga mamimili ay kailangang magsaliksik, magpondo, bumili, maglagay ng tauhan, maglatag, at subaybayan ang karagdagang **mga produktong pang-seguridad** upang mabawasan ang pagkakataong makompromiso. Ang mga maliliit at katamtamang laki na mga organisasyon (SMO) ay karaniwang hindi nagagawang pangasiwaan ang mga opsyong ito. Nahaharap sila sa kakulangan sa kadalubhasaan, pagpopondo, at oras na nagbubuwis sa bandwidth at paggana, na pinipilit ang seguridad sa isang mas mababang priyoridad, at, sa kabuuan, nagpapalala ng kolektibong panganib. Sa kabaligtaran, ang mga pamumuhunan sa seguridad ng kaunting mga tagagawa ay lalago. Ang isang karaniwang parirala na nagbubuod sa problema ay ang industriya ng software ay nangangailangan ng mas ligtas na mga produkto, hindi magdaragdag pa ng mga produktong pang-seguridad. Dapat pangunahan ng mga tagagawa ng software ang pagbabagong iyon.

> ***Ang industriya ng software ay nangangailangan ng mas ligtas na mga produkto, hindi higit pang mga produkto ng seguridad. Dapat pangunahan ng mga tagagawa ng software ang pagbabagong iyon.***

Ngayon, minsan ay nagbabasa kami ng mga komento mula sa mga tagagawa na nagpapaliwanag na ang isang mamimili ay nakompromiso dahil sa hindi pag-enable ng isang partikular na katangian ng seguridad o pagsunod sa partikular na gabay sa pagpapatigas. Sa halip, pagkatapos ng isang kompromiso, dapat ipaliwanag ng mga tagagawa kung ang isang partikular na katangian sa seguridad o partikular na gabay sa hardening ay pumigil sa kompromiso at isaalang-alang na gawin itong default nang walang bayad. Sa mga kasong iyon kung saan ang produkto mismo ay hindi sapat na pinatigas sa mga yugto ng disenyo at pagpapatupad, dapat ipaliwanag ng tagagawa kung paano nila ginagawa upang alisin ang klase ng kahinaan mula sa kanilang mga linya ng produkto.

Ang mga tagagawa ng software ay may responsibilidad na tiyakin na ang kanilang mga produkto ay idinisenyo at binuo nang may seguridad bilang pangunahing priyoridad. Sa layuning iyon, dapat nilang **matutong sukatin ng walang kinikilingan ang mga resulta** ng kanilang mga pagsisikap sa larangan. Nananawagan kami sa mga tagagawa na hindi lamang tumuon sa kanilang mga panloob na pagsisikap, ngunit sa layuning sukatin at regular na iulat ang mga resulta at pagiging epektibo ng mga pagsusumikap sa seguridad at pagsasaayos ng isang produkto, at upang bumuo ng isang feedback loop na lumilikha ng mga pagbabago sa SDLC na humahantong sa masusukat na mga pagpapabuti sa kaligtasan ng mamimili at mas ligtas na mga produkto. Ang pag-uulat ay dapat magsama ng hindi nakikilalang datos na magagamit ng komunidad ng pananaliksik sa akademiko at seguridad upang subaybayan ang mga uso sa mataas na antas at sukatin ang pag-unlad ng ekosistema sa kabuuan.

PAGPAPAKITA NG PRINSIPYO NA ITO

Ang mga tagagawa ng software at mga online na serbisyo ay dapat maghanap ng mga paraan upang ipakita ang mga tagumpay sa pagpapatupad ng prinsipyong ito. Dapat silang magbigay ng ebidensya sa anyo ng mga artifact para masuri ng mga tagalabas. Walang isang artifact mismo ang magpapatunay na ang isang tagagawa ay nagpapatupad ng isang matatag na programa na secure by design, ngunit sa pamamagitan ng pagbibigay ng iba't ibang mga artifact (gawa ng tao) ay magpapakita sa pangako ng tagagawa sa pagbuo ng mga ligtas na produkto. Ang pamamaraang ito ay nasa diwa ng "ipakita, sa halip na sabihin."

Upang ipakita ang prinsipyong ito, dapat isaalang-alang ng mga tagagawa ng software ang mga hakbang gaya ng nasa sumusunod na listahan. Kinikilala ng mga organisasyong may-akda na kakaunti ang mga tagagawa ng software ang magagawang agad na ipatupad ang mga kasanayang ito at makagawa ng kaukulang mga artifact sa simula ng kanilang pagpapatupad ng secure by design. Dagdag pa, kakailanganin ng mga tagagawa ng software na unahin ang listahang ito depende sa kung paano i-deploy ng mga mamimili ang produkto sa field upang makamit ang pinakamalaking benepisyo sa seguridad.

SECURE BY DEFAULT NA MGA KASANAYAN

1. **Tanggalin ang mga default na password.** Patuloy na idinadawit ang mga default na password bilang sanhi ng maraming pag-atake bawat taon. Ang paggawa ng pangako na alisin ang talamak na problemang ito ay hihinto sa madaling pagkonekta ng mga umaatake. Katulad nito, dapat isaalang-alang ng mga tagagawa kung anong mga kasanayan sa password ang dapat ipatupad, tulad ng pinakamababang haba ng password at hindi pinapayagan ang mga kilalang napasok na password.

2. **Magsagawa ng mga pagsubok sa larangan.** Habang patuloy na umuunlad at nagiging mas kumplikado ang teknolohiya, lalong mahalaga para sa mga tagagawa ng software na magsagawa ng pagsubok sa user na nakasentro sa seguridad upang maunawaan ang postura ng seguridad ng kanilang mga produkto sa larangan. Katulad ng kung paano ipinapaalam ng pananaliksik ng user ang mga kinakailangan sa paggawa ng software, dapat ding magsagawa ng pananaliksik ng gumagamit na nakatuon sa seguridad ang mga tagagawa ng software upang maunawaan kung saan kulang ang security user experience (UX). Sa pamamagitan ng pag-obserba kung paano mailagay at gagamitin ng mga mamimili ang kanilang mga produkto sa mundo, maaaring makakuha ang mga tagagawa ng software ng mahahalagang pag-unawa sa kakayahang magamit at pagiging epektibo ng kanilang mga katangian at kontrol sa seguridad. Makakatulong ang mga insight na ito na matukoy ang mga lugar para sa pagpapabuti at pinuhin ang kanilang mga produkto upang mas mahusay na matugunan ang mga pangangailangan sa seguridad ng mga mamimili. Halimbawa, ang mga pagsubok sa larangan ay maaaring magmungkahi ng mga pagbabago sa daloy ng UX, mga default, pag-alerto, at pagsubaybay. Maaari ding ipakita ng mga field test kung saan binabawasan ng mga nakaraang pagpapahusay sa disenyo ng produkto ang bilis ng mga patch ng seguridad, binabawasan ang mga error sa pagsasaayos, at pinapaliit ang attack surface.

Dapat isaalang-alang ng mga tagagawa ang sumusunod:

- Tama bang ipinapatupad ng mga mamimili ang gabay sa pagpapatigas?
- Nakakatupad ba ang mga kasalukuyang katangian ng seguridad ng produkto gaya ng inaasahan sa larangan?
- Talagang lumalaban ba ang mga katangian na iyon sa mga pag-atake sa totoong mundo?
- Aling mga katangian ang mas makakabawas sa posibilidad ng kompromiso?

Tandaan: Upang makakuha ng mas malalim na mga insight sa mga elementong ito, maaaring naisin ng mga tagagawa ng software na makipagsosyo sa mga mamimili upang magsagawa ng mga ehersisyo ng red team upang makita kung paano lumalaban ang produkto sa mga pag-atake. Maaaring maganap sa mga pagsuri sa larangan na ito sa pisikal na lugar ng mamimili, virtual, o sa pamamagitan ng telemetry mula sa application sa paraang pinapanatili ang pagkapribado.

3. **Bawasan ang laki ng gabay sa pagpapatigas.** Maaaring pahusayin ng mga tagagawa ang mga tindig ng seguridad ng mga mamimili sa pamamagitan ng pag-streamline o kahit na pag-aalis ng mga gabay sa pagpapatigas ng produkto at pagtutuon sa mga pinakamahalagang hakbang sa seguridad na dapat bigyang-priyoridad ng mga mamimili kapag naglalagay ng kanilang mga produkto. Sa halip na ibaon ang mga mamimili sa listahan ng mga gawaing pangseguridad, dapat na tukuyin ng mga tagagawa ang mga nangungunang panganib sa seguridad na madaling kapitan ng kanilang mga produkto at magbigay ng malinaw at maigsi na patnubay sa kung paano pagaanin ang mga panganib na ito. Dagdag pa, dapat bigyan ng mga tagagawa ang mga mamimili ng mga gamit at automation na nagpapadali sa proseso ng pagpapatupad ng mga kontrol sa seguridad, tulad ng mga script na madaling ilatag sa kanilang kapaligiran. Ang mga gamit na ito ay dapat ding makapagpatunay at malinaw na maipakita ang mga pagbabagong ginawa mula sa orihinal na baseline. Sa pamamagitan ng pag-streamline ng mga gabay sa hardening at pagbibigay sa mga mamimili ng madaling gamitin na mga gamit at automation, maaaring bawasan ng mga tagagawa ang pasanin sa kanilang mga mamimili at tumulong na matiyak na ang kanilang mga produkto ay nailatag sa isang ligtas na paraan. Ang isang taktika ay ang pag-isipang ipatupad ang prinsipyo ng Pareto upang bawasan ang bilang ng mga hakbang para sa mga karaniwang kaso ng paggamit (ang 80%), at pagkatapos ay magbigay ng gabay at gamit sa konteksto para sa hindi gaanong karaniwang mga sitwasyon (ang 20%). Sa ganitong paraan, gagawing madali ng mga tagagawa ng software ang mga paggawa ng mga simpleng

bagay, at posible ang mahihirap na bagay. Ang field testing ay magiging isang mabisang gamit sa pagsukat kung gaano katagal matuklasan, maunawaan, at ipatupad ng mga mamimili ang mga gabay sa pagpapatigas. Dapat isaalang-alang ng mga tagagawa kung paano maaaring hikayatin ng produkto ang mga administrator na gumawa ng aksyon sa loob ng produkto mismo sa halip na umasa sa kanila upang ipatupad ang mga gawain mula sa isang gabay sa pagpapatigas.

4. **Aktibong iwasan ang paggamit ng mga hindi ligtas na legacy na katangian.** Unahin ang seguridad sa pamamagitan ng malinaw na mga landas sa pag-papahusay kaysa sa mga pabalik na pagkakatugma. Maglathala ng mga post sa blog na nagpapakita ng paggamit ng mga mas ligtas na katangian at protocol, at ihinto ang paggamit ng mga hindi ligtas na katangian sa pamamagitan ng anunsyo, posibleng mula sa mismong produkto. Malaking bilang ng mga mamimili ang nagpakita na hindi nila papanatilihing napapanahon ang kanilang mga sistema gamit ang modernong network, pagkakakilanlan, at iba pang kritikal na katangian ng seguridad. Sa ilang mga kaso, natatakot ang mga mamimili na masira ang kasalukuyang functionality sa isang pagpapahusay. Sa pamamagitan ng paggawa ng mga pag-upgrade na walang gambala, malamang na mag-upgrade ang mga mamimili at makakuha ng mga pag-aayos sa seguridad nang mas madalas at mabilis. Ang mga tagagawa ng software ay dapat na agresibong itulak ang mga mamimili sa mga daanan ng pag-upgrade na nagpapababa sa panganib ng mamimili.

5. **Ipatupad ang mga agaw-pansin na alerto.** Katulad ng mga chime ng seat belt sa mga kotse na patuloy na gumagawa ng ingay kapag hindi nakakabit ang mga seat belt, dapat na ipatupad ng mga tagagawa ang napapanahon at paulit-ulit na mga alerto kapag ang mga user o admin ay nasa tunay na hindi ligtas na estado, na nagbabala sa mga administrator na sila ay gumagamit ng hindi na ginagamit na mga magkasunud-sunod nagawain sa kanilang mga kapaligiran at nagmumungkahi ng mga landas sa pagpapahusay. Ipatupad ang napapanahon at paulit-ulit na pag-aalerto kapag ang mga gumagamit o namamahala, o ang pagsasaayos ng aplikasyon, ay nasa hindi ligtas na estado. Gawing regular at malinaw sa mga administrador ang hindi ligtas na modo. Maaaring mangailangan ng karagdagang katangian ang isang super administrator na kilalanin ang kakulangan ng MFA sa kanilang kuwenta sa bawat pag-login, o kahit na huwag paganahin ang ilang pangunahing katangian hanggang sa paganahin nila ang MFA. May puwang upang makamit ang mga layuning ito habang hindi lumilikha ng pagkapagod sa alerto.

6. **Gumawa ng mga ligtas na template ng pagsasaayos.** Maaaring i-preset ng mga template na ito ang ilang partikular na pagsasaayos sa mga ligtas na setting batay sa risk appetite ng isang organisasyon. Bagama't maaaring napakasimpleng magkaroon ng mababang/katamtaman/mataas na mga template ng seguridad, ang halimbawang iyon ay naglalarawan kung gaano karaming mga setting ang maaaring baguhin upang pamahalaan ang panganib para sa organisasyon. Ang mga template ay maaaring suportahan ng mga gabay sa pagpapatigas sa mga panganib na natukoy ng tagagawa.

LIGTAS NA MGA KASANAYAN SA PAGBUBUO NG PRODUKTO

1. **Pagsunod sa dokumento sa isang ligtas na SDLC framework.** Ang mga ligtas na SDLC framework ay nagbibigay ng mga layunin at halimbawa sa mga tao, proseso, at teknolohiya. Isaalang-alang ang paglathala ng isang detalyadong paglalarawan kung aling mga ligtas na SDLC framework control ang ipinatupad at ilarawan ang anumang mga alternatibong kontrol na ginamit. Sa loob ng US, isaalang-alang ang paggamit ng NIST Secure Software Development Framework (SSDF). Bagama't hindi isang checklist, ang SSDF ay "naglalarawan ng isang hanay ng mga pangunahing, mahusay na kasanayan para sa ligtas na software development."

2. **Idokumento ang Mga Layunin sa Pagganap ng Cybersecurity (CPG) o katumbas na pagsunod.** Kapag pinatunayan ng isang organisasyon na sumusunod sila sa pamantayan ng NIST SSDF, iginigiit nila na ang kanilang SDLC ay sumusunod sa pinakamahuhusay na kagawian. Gayunpaman, hindi sapat para sa kanila na magkaroon lamang ng matatag na SDLC. Kailangan din nilang protektahan ang sarili nilang kapaligiran sa pagpapatubo at pag-unlad mula sa mga malisyosong aktor na gustong manipulahin ang mga katangian ng seguridad ng produkto habang nasa pag-uunlad pa ito. Ito ay hindi isang teoretikal na klase ng pag-atake, ngunit isa na natupad na may masamang epekto sa mga mamimili, at sa pamamagitan ng pagpapalawig ng pambansang seguridad. Dapat isaalang-alang ng mga organisasyon ang paglathala ng mga detalye sa pagsunod ng organisasyon sa mga CISA CPG, NIST Cybersecurity Framework (CSF), o iba pang mga framework ng programa sa cybersecurity.

3. **Pamamahala ng kahinaan.** Ang ilang mga tagagawa ay may programa sa pamamahala ng kahinaan na tumutuon sa pag-patch ng mga kahinaan na natuklasan sa loob o panlabas, at iba pa. Ang mga mas mature na programa ay nagsasama ng malawak na data-driven na pagsusuri ng mga kahinaan at ang mga ugat ng mga ito, na nagsasagawa ng mga hakbang upang sistematikong alisin ang buong klase ng kahinaan[3]. Nagpapatupad sila ng mga pormal na programa sa paligid ng pagtatakda ng pagpaplano ng kalidad, kontrol sa kalidad, pagpapabuti ng kalidad, at pagsukat ng kalidad. Tinitingnan nila ang pamamahala ng depekto bilang isang bagay sa negosyo, hindi lamang isang bagay sa seguridad. Ang mga programang ito ay hindi magkaiba sa ilang mga paraan sa kalidad at kaligtasan ng mga programa sa ibang mga industriya.

4. **Responsableng gumamit ng open source software.** Kapag ginamit ang open source na software, maging responsable sa pamamagitan ng pagsusuri sa mga lantad na mapagkukunan na, payamanin ang mga kontribusyon sa code na pabalik sa mga nangangailangan, at pagtulong na mapanatili ang pagbuo at pagpapanatili ng mga kritikal na bahagi. Para sa sanggunian, ang Ministry of Economy, Trade, and Industry (METI) ng Japan ay naglathala ng "Koleksyon ng Mga Halimbawa ng Kaso ng Paggamit Tungkol sa Pamamaraan ng Pamamahala para sa Paggamit ng OSS at Pagtiyak ng Seguridad Nito." (Collection of Use Case Examples Regarding Management Methods for Utilizing OSS and Ensuring Its Security)

5. **Magbigay ng mga ligtas na default para sa mga developer.** Gawing ligtas ang default na ruta sa panahon ng paggawa ng software sa pamamagitan ng pagbibigay ng mga ligtas na building block para sa mga developer. Halimbawa, dahil sa paglaganap ng mga kahinaan ng SQL injection na nagdudulot ng pinsala sa totoong mundo, tiyaking gumagamit ang mga developer ng isang mahusay na pinapanatili na library upang maiwasan ang klase ng kahinaan. Kilala rin bilang "mga sementadong kalsada" o "mga landas na may maliwanag na ilaw," tinitiyak ng kasanayang ito ang parehong bilis at seguridad, at binabawasan ang pagkakamali ng tao.

6. **Palaguhin ang isang tagapaglikhang mga manggagawa ng software na nakakaunawa sa seguridad.** Tiyaking nauunawaan ng iyong mga developer ng software ang seguridad sa pamamagitan ng pagsasanay sa kanila sa mga ligtas na pinakamahuhusay na kagawian sa coding. Dagdag pa, tumulong na baguhin ang mas malawak na workforce sa pamamagitan ng pag-update ng mga kasanayan sa pag-hire upang suriin ang kaalaman sa seguridad at pakikipagtulungan sa mga unibersidad, kolehiyo ng komunidad, bootcamp, at iba pang mga tagapagturo upang isama ang seguridad sa mga kurikulum sa computer science at software development.

[3] NIST SSDF, PO 1.2, Halimbawa 2: "Tukuyin ang mga patakarang tumutukoy sa mga kinakailangan sa seguridad para sa software ng organisasyon, at i-verify ang pagsunod sa mga pangunahing punto sa SDLC (hal., mga klase ng mga bahid ng software na na-verify ng mga gate, mga tugon sa mga kahinaan na natuklasan sa inilabas na software)."

7. **Subukin ang security incident event management (SIEM) at security orchestration, automation, and response (SOAR) integration.** Bilang karagdagan sa pagsasagawa ng mga field test, makipagtulungan sa mga sikat na provider ng SIEM at SOAR kasabay ng mga piling mamimili upang maunawaan kung paano gumagamit ng mga log ang mga pangkat sa pagtugon sa insidente upang maimbestigahan ang pinaghihinalaan o totoong mga insidente sa seguridad. Ilang software developer ang may karanasan sa pagtugon sa isang insidente at maaaring gumawa ng mga log entry na hindi nakakatulong sa mga sasaklolo gaya ng inaasahan nila. Sa pamamagitan ng pakikipag alyansa sa mga teknolohiya ng SIEM at SOAR at mga propesyonal sa pagtugon sa totoong insidente, ang pangkat ng manlilikha ay makakagawa ng mga log na nagsasabi ng tama at kumpletong kuwento, nakakatipid ng oras at nakakabawas ng kawalan ng katiyakan sa panahon ng isang insidente.

8. **Ihanay sa Zero Trust Architecture (ZTA).** Ihanay ang mga gabay sa pag-deploy ng produkto sa, halimbawa, mga modelo ng NIST ZTA at ang CISA Zero Trust Maturity Model. Hikayatin ang mga mamimili na isama ang mga prinsipyong ito sa kanilang mga kapaligiran.

MGA GAWAIN PARA SA SEGURIDAD NG NEGOSYO

1. **Magbigay ng pag-log nang walang karagdagang bayad.** Ang mga serbisyo ng Cloud ay dapat na mangako sa pagbuo at pag-iimbak ng mga log na nauugnay sa seguridad nang walang karagdagang bayad. Ang mga nasasakupang produkto ay dapat ding bumuo ng mga log na nauugnay sa seguridad nang walang karagdagang bayad. Dagdag pa, ang produkto ay dapat mag-log ng mga kaganapan sa seguridad bilang default dahil maraming mga mamimili ang maaaring hindi maunawaan ang kanilang halaga hanggang pagkatapos ng isang insidente. Ang mga taktika na ito ay maaaring mangailangan ng masusing pagsusuri tungkol sa kung anong mga kaganapang pangseguridad ang dapat i-log upang magbigay ng kaalaman sa estado ng cybersecurity, kung paano maaaring isaayos ng isang mamimili ang pag-log, para sa kung anong yugto ng panahon ang mga log ay pinananatili, kung paano pinoprotektahan ang integridad ng log at imbakan, at kung paano masusuri ang mga log. Sa ilang mga kaso, ang pagsusuri ay maaaring magmungkahi ng pangangailangan para sa isang refactoring ng arkitektura ng pamamahala ng log ng application upang makatulong na gawing na-aaksyonan ang mga ito at sa gastos na kaya ng tagagawa. Ang pakikipagtulungan sa mga eksperto sa pagtugon sa insidente (IR) ay maaaring magpataas ng mga pagkakataon na ang mga log ay magiging kapaki-pakinabang sa mga imbestigador sa field. Tingnan ang seksyon sa mga SIEM.

2. **Alisin ang mga nakatagong buwis.** Maglathala ng pangako na hindi kailanman maniningil para sa mga katangian sa seguridad, privacy o pagsasama. Halimbawa, sa loob ng mas malaking saklaw ng identity and access management (IAM), may mga serbisyong tinatawag na single sign-on (SSO) services. Ang ilang mga tagagawa ay naniningil nang higit pa upang ikonekta ang kanilang sistema sa isang serbisyo ng SSO (minsan ay tinutukoy bilang isang tagapagbigay ng pagkakakilanlan). Itong “SSO tax” ay nangangahulugan na ang mabuting pagkakakilanlan at pamamahala sa pag-access ay hindi maabot ng maraming SMO, na pumipigil sa kanila na makamit ang isang malakas na postura ng seguridad. Ang ilang mga serbisyo ay naniningil nang higit pa upang paganahin ang MFA para sa mga user. **Ang seguridad ay hindi dapat mapresyuhan bilang isang luxury good ngunit ituring na karapatan ng mamimili.** Nangatuwiran ang ilang mga tagagawa na kakaunti ang mga mamimili na humihiling ng mga katangian na ito, at mas mahal ang mga ito sa pagmementena. Binabalewala ng mga argumentong ito ang katotohanang kakaunting mamimili ang tatawag para magreklamo o makipagtawaran, hindi lahat ng mamimili ay talagang nauunawaan kung ano ang mga pakinabang ng mga katangian na ito, at ang lahat ng katangian ay nagkakahalaga para mamentena. Gayunpaman, wala kaming nakikitang maraming tagagawa na naniningil ng dagdag para sa availability o integridad ng datos. Ang mga gastos para suportahan ang mga pangunahing katangiang iyon ay kasama sa presyong binabayaran ng lahat ng mamimili, katulad ng mga gastos sa pagsasama ng mga seatbelt, collapsible steering column, at airbag na nagliligtas ng mga buhay sa mga aksidente.

3. **Tanggapin ang mga bukas na pamantayan.** Ipatupad ang mga bukas na pamantayan, lalo na sa mga karaniwang network at mga protocol ng pagkakakilanlan. Iwasan ang mga proprietary protocol kapag available ang mga bukas na pamantayan.

4. **Magbigay ng upgrade tooling.** Maraming mga mamimili ang nag-aatubili na gamitin ang pinakabagong bersyon ng produkto, kabilang ang pag-deploy ng mas bago at mas ligtas na mga katangian tulad ng mga ligtas na koneksyon sa network. Maaaring pataasin ng mga tagagawa ng software ang pag-aampon ng mamimili ng mga bagong upgrade sa pamamagitan ng pagbibigay ng tooling upang makatulong na mabawasan ang kawalan ng katiyakan at panganib. Mag-alok ng mga libreng lisensya para sa mga mamimili na subukan ang mga upgrade at patch sa isang pagsubok na kapaligiran bilang isang paraan upang hikayatin ang mga mamimili.

PRINSIPYO 2: Tanggapin ang Radikal na Katapatan at Pananagutan

PALIWANAG

Dapat ipagmalaki ng mga tagagawa ng software ang kanilang sarili sa paghahatid ng mga ligtas at secure na produkto, pati na rin ang pagkakaiba sa kanilang sarili mula sa iba pang komunidad ng tagagawa batay sa kanilang kakayahang gawin ito.

Tugunan natin ang isang karaniwang alalahanin tungkol sa katapatan. Kapag tinatalakay ng mga gumagamit ang radikal na katapatan, may posibilidad na magulo ang pag-uusap dahil sa pag-aalaala na nagbibigay sila ng "roadmap para sa mga umaatake." Gayunpaman, may maraming ebidensya na ang mga umaatake ay gumagana nang maayos nang walang ganoong mga roadmap, at ang mga naturang alalahanin ay dapat na bumalik sa katapatan na nakikinabang sa mga direktang mamimili, hindi direktang mamimili, ugnayan sa pagtustos, at buong industriya ng software.

Tinutulungan ng katapatan ang industriya na magtatag ng mga kadalasang gawi ng paggawa—sa madaling salita, kung ano ang hitsura ng "maganda". Tinutulungan nito ang mga kombensyong iyon na magbago sa paglipas ng panahon bilang tugon sa mga pangangailangan ng mamimili, mga pagbabago sa mga taktika ng aktor sa pagbabanta o ekonomiya, o pag-unsad ng teknolohiya. Tinutulungan ng katapatan ang mga tagagawa na may mas kaunting mapagkukunan na matuto mula sa mga may mas mature at may kakayahang mapagkukunan. Ang mga pag-uusap tungkol sa pagbabahagi ng impormasyon ay dapat lumampas sa mga real-time na tagapagpahiwatig ng pagbabanta, upang isama ang mga elemento sa ibaba.

Pinipilit ng katapatan na gawin ang mga desisyon tungkol sa seguridad nang maaga sa proseso ng pagbuo, at maging tuluy-tuloy na aktibidad ng mga lider ng negosyo pati na rin ng mga inhinyero at propesyonal sa seguridad. Ang katapatan ay bumubuo ng pananagutan sa produkto.

Isang tala sa pagpili ng pang-uri na "radikal" sa harap ng "katapatan." Sa ngayon, bihira para sa mga tagagawa ng software na mag-lathala ng detalyadong impormasyon tungkol sa kung paano sila bumuo at nagpapanatili ng software at kung paano nila pinalalaki ang kanilang mga programa gamit ang datos sa paglipas ng panahon. Sa industriya ng software, ilang mga tagagawa ang nag-aalok ng mga guided tour kung paano nila idinisenyo ang kanilang software. Mayroong ilang mga pagkakataon para sa mga tagagawa ng software na makita kung paano binubuo ng mga kaparehong organisasyon ang kanilang mga SDLC program, at kung paano nananatili ang mga programa na iyon sa mga kapaligiran ng mamimili laban sa mga tunay na umaatake. Ang kolektibong industriya ay makikinabang mula sa higit pang pagbabahagi ng impormasyon sa mga paksa tulad ng mga diskarte upang sukatin ang halaga ng mga depekto sa seguridad at upang maalis ang mga klase ng kahinaan. Bilang resulta ng mga karaniwang kasanayang ito, dapat matutunan ng bawat tagagawa ng software kung paano haharapin ang seguridad ng produkto nang mag-isa. Marahil sa pamamagitan ng hindi paglalagay ng marangyang buwis sa mga tampok na pangseguridad, ang kaligtasan at seguridad samakatuwid ay nagiging sentro ng gastos sa halip na sentro ng tubo, at makikinabang ang mga kumpanya sa pamamagitan ng pagpapagaan ng kargada sa pamamagitan ng pakikipagtulungan at katapatan.

Gusto naming tumuon sa mga taktika na materyal na magpapabilis sa ebolusyon ng industriya ng software. Hindi na namin kayang gumawa ng oportunistikong karagdagang pagpapabuti. Kung sama-sama nating malalagpasan ang mga banta ng matatalino at madaling makibagay na mga kalaban, dapat nating yakapin ang mga antas ng katapatan na hindi komportable ngayon, na magpapasulong sa industriya. May mga tagagawa ngayon na sumusunod sa mga prinsipyo ng secure by design. Tulad ng sinabi ni William Gibson, "narito na ang hinaharap, hindi ito masyadong pantay na ipinamamahagi." **Ang radikal na katapatan ay makakatulong na ipamahagi ang impormasyong iyon at mas makinabang ang mga tagapagtanggol kaysa sa aming mga kalaban.**

Higit pa ang magagawa ng katapatan kaysa sa pagtulong sa mga kaparehong organisasyon na maging mature ang kanilang mga SDLC. Ang mga inaasahang mamimili at mamumuhunan ay maaaring matuto nang higit pa tungkol sa mga pamumuhunan at tradeoff na ginawa ng mga tagagawa, at ang postura ng seguridad na ginawa ng mga pamumuhunan na iyon para sa mga mamimili. Ang mga tagagawa na tumanggap ng radikal na katapatan ay magbibigay sa mga mamimili ng impormasyon upang matulungan silang gumawa ng mga desisyon sa pagbili hindi lamang sa presyo at mga katangian, ngunit sa seguridad din.

Kung gaano kahirap ang mga organisasyon na nagsisikap na maging ligtas ang kanilang supply chain at ang kanilang SDLC, may mga kumpanya na nakompromiso ang kanilang mga proseso sa pagtatayo nitong bago lang. Ang pagtanggap sa radikal na katapatan ay dapat humantong sa pagsisiwalat sa publiko ng pag-atake pati na rin ang mga pagpapahusay na ginawa ng kumpanya upang maiwasan at matukoy ang mga pag-atake sa hinaharap. Ang paraan ng pagbabahagi ng impormasyon ay makakatulong sa ibang mga organisasyon na matuto nang hindi kinakailangang magdusa ng parehong kapalaran.

PAGPAPAKITA NG PRINSIPYO NA ITO

Upang ipakita ang prinsipyong ito, ang mga tagagawa ng software ay dapat gumawa ng mga hakbang kabilang ang mga sumusunod:

SECURE BY DEFAULT NA MGA KASANAYAN

1. **Maglathala ng pinagsama-samang seguridad na may kaugnayang istatistika at trend.** Kabilang sa mga halimbawang paksa ang pagpapatibay ng MFA ng mga mamimili at administrator at paggamit ng mga hindi ligtas na legacy na protocol.
2. **Ilathala ang mga istatistika ng patching.** Idetalye kung ilang porsyento ng mga mamimili ang nasa pinakabagong bersyon ng produkto, at kung ano ang iyong ginagawa upang gawing mas madali at mas maaasahan ang mga pagbabago.
3. **Maglathala ng datos sa mga hindi nagamit na pribilehiyo.** Maglathala ng pinagsama-samang impormasyon sa labis na mga pahintulot sa iyong mamimili pati na rin ang mga pagtulak at iba pang pagbabago sa produktong ginagawa mo upang mabawasan ang mga pag-atake ng mga mamimili. Ang mga hindi nagamit na pribilehiyong ito ay malamang na maging mahusay na mga kandidato para sa mga alerto ng administrator, tulad ng seatbelt chimes.

MGA KASANAYAN PARA SA LIGTAS NA PAGLIKHA NG PRODUKTO

1. **Magtatag ng mga panloob na kontrol sa seguridad.** Maraming kumpanya ang nakakita ng mga benepisyo ng paglipat ng kanilang datos sa mga cloud provider. Ngayon ang mga cloud provider na iyon ay naging target ng mga umaatake. Dapat maglathala ang mga provider ng Software as a Service (SaaS) na mga istatistika ng kanilang mga panloob na kontrol. Halimbawa, ang mga tagapagbigay ng SaaS ay dapat maglathala ng mga istatistika sa kanilang panloob na pagkakatalaga ng phishing-resistant MFA, katulad ng Fast Identity Online (FIDO) na pagpapatunay. Sa isip, dapat nilang sabihin na walang miyembro ng kawani ang makakakuha ng mamimili o iba pang sensitibong datos nang hindi nagpapatunay sa pamamagitan ng MFA na lumalaban sa phishing.

2. **Maglathala ng mga modelo ng pagbabanta sa mataas na antas.** Ang mga produktong secure by design ay nagsisimula sa mga nakasulat na modelo ng pagbabanta na naglalarawan kung ano ang sinusubukang protektahan ng mga tagalikha at kung kanino. Ang mga epektibong modelo ng pagbabanta ay nababatid sa kung paano nangyayari ang mga panghihimasok sa mundo, at dapat na sumasakop sa parehong enterprise at development environment, pati na rin ang paraan na nilalayon ng mga tagagawa ng software na gamitin ito sa mga environment ng mamimili.

3. **Maglathala ng mga detalyadong ligtas na SDLC self-attestations.** Ang mga tagagawa na sumusunod sa NIST SSDF, o iba pang katulad na mga framework ay aktibong nagtatrabaho patungo sa isang mature na lifecycle ng pagbuo ng software. Ang paglathala ng self-attestation kung anong mga kontrol ang pinatibay ng tagagawa, at para sa kung aling mga produkto, ay magpapakita ng pangako sa pagsunod sa mga pinakamahuhusay na kagawian na ito at magbibigay ng mas mataas na antas ng kumpiyansa sa kanilang mga mamimili. Halimbawa sa iba pang mga pamaraan ng sertipikasyon ay ang Israel Cyber Supply Chain Methodology.

4. **Tanggapin ang katapatan ng kahinaan.** Maglathala ng pangako na magtitiyak na ang mga natukoy na kahinaan sa produkto ay mailathala bilang mga entry sa CVE na tama at kumpleto. Mas totoo pa ito lalo na para sa field ng Common weakness enumeration na tumutukoy sa ugat ng mga kahinaan. Kung mas tama at kumpleto ang pampublikong CVE database, mas masusubaybayan ng industriya kung paano nagiging mas ligtas ang mga produkto, at kung aling mga klase ng mga kahinaan ang pinakalaganap. Gayunpaman, mag-ingat sa tuksong bilangin ang mga CVE bilang negatibong sukatan, dahil ang mga bilang na ito ay tanda din ng isang malusog na pagsusuri ng code at komunidad ng pagsubok. Habang nagpapatupad ang mga tagagawa ng pilosopiyang secure by design, posibleng sa una ay tataas ang kanilang raw CVE count dahil sa mas komprehensibong pagtuklas at remediation ng mga kahinaan sa umiiral na code. Dapat maglathala ang mga tagagawa ng pagsusuri ng mga nakaraang kahinaan, kabilang ang anumang mga pattern at hakbang na ginawa upang matugunan ang buong klase ng mga kahinaan. Halimbawa, kung ang malaking porsyento ng mga CVE ng kumpanya ay nauugnay sa cross-site scripting (XSS), ang pagdodokumento sa root cause analysis, tugon (katulad ng paglipat sa mga web template frameworks na pumipigil sa XSS), at mga resulta ay magsenyas sa mga mamimili na sila ay hindi mabibiktima ng isang klase ng kahinaan kung saan ang mga pagpapagaan ay naiintindihan sa loob ng ilang mga dekada.

5. **Ilathala ang Software Bills of Materials (SBOMs).** Dapat ay maatasan ng mga tagagawa ang kanilang mga supply chain. Dapat bumuo at magpanatili ang mga organisasyon ng mga SBOM [2] para sa bawat produkto, humiling ng datos mula sa kanilang mga supplier, at gawing available ang mga SBOM para sa mga downstream na mamimili at gumagamit. Makakatulong ito na ipakita ang kanilang kasipagan sa pag-unawa sa mga bahaging ginagamit nila sa paggawa ng kanilang mga produkto, ang kanilang kakayahang tumugon sa mga bagong natukoy na panganib, at makakatulong sa mga mamimili na maunawaan kung paano tumugon kung ang isa sa mga module sa supply chain ay may bagong natagpuang kahinaan.

Bilang sanggunian, inilathala ng Ministry of Economy, Trade, and Industry (METI) ng Japan ang "Gabay sa Pagpapakilala ng Software Bill of Materials (SBOM) para sa Pamamahala ng Software." Dapat umabot ang katapatan sa firmware sa mga nakalagay na aparato at ang datos at mga modelong ginagamit sa AI/machine learning (ML). Higit pa sa pagtulong sa mga desisyon sa pagbili at mga kakayahan sa pagpapatakbo, ang mga SBOM ay may mahalagang papel sa imprastraktura upang matukoy at tumugon sa mga nakakahamak na pag-atake sa supply chain.

6. **Maglathala ng patakaran sa pagsisiwalat ng kahinaan.** Maglathala ng patakaran sa pagsisiwalat ng kahinaan na (1) nagpapahintulot sa pagsubok laban sa lahat ng produktong inaalok ng tagagawa at mga kundisyon para sa mga pagsubok na iyon, (2) nagbibigay ng legal na ligtas na daungan para sa mga aksyon na isinagawa alinsunod sa patakaran, at (3) nagbibigay-daan sa pampublikong pagsisiwalat ng mga kahinaan pagkatapos ng isang itinakdang timeline. Ang mga tagagawa ay dapat magsagawa ng root-cause analysis ng mga natuklasang kahinaan at, hanggang sa makakaya, gumawa ng mga aksyon upang alisin ang buong mga klase ng kahinaan. Tingnan ang Template ng Patakaran sa Pagbubunyag ng Vulnerability ng CISA para sa reference na wika.

MGA KASANAYAN PARA SA SEGURIDAD NG NEGOSYO

1. **Pangalanan sa publiko ang isang secure by design na senior executive sponsor.** Sa maraming organisasyon, ang seguridad (tulad ng kalidad) ay itinalaga sa mga teknikal na koponan na may limitadong kakayahan na gumawa ng mga pagbabago sa istruktura upang kapansin-pansing mapabuti ang seguridad ng mga produkto. Ang pampublikong pagbibigay ng pangalan sa isang nangungunang executive ng negosyo upang pangasiwaan ang secure by design program ay magpapabago sa seguridad ng mga produkto na magiging isang mataas ang lebel na alalahanin sa negosyo.

2. **Maglathala ng secure by design roadmap.** Dapat idokumento ng mga tagagawa ang mga pagbabagong ginawa sa kanilang SDLC para mapahusay ang seguridad ng mamimili, kabilang ang mga detalye tungkol sa mga ulat sa field-test, mga pagkilos na ginawa upang maalis ang buong klase ng kahinaan, at iba pang mga item na nakalista sa iba pang mga prinsipyo. Tulad ng sa kaso ng mga pagsisikap sa pagpapahusay ng kalidad, ang mga programa sa pagpapahusay ng seguridad ay may natatanging mga yugto ng pagpaplano, kontrol, at pagpapabuti. Sa diwa ng pagpapakita sa halip na pagsasabi, ang paglathala ng roadmap at ang mga detalye sa likod ng mga yugtong ito ay bubuo ng kumpiyansa na ang mga produkto ay ligtas sa pamamagitan ng disenyo. Pagkatapos makamit ang makabuluhang pag-unlad, maaaring maidetalye ng mga tagagawa ang mga ito sa mga ulat ng katapatan. Ang paggawa nito ay hindi lamang nagpapakita ng pagsunod sa secure by design na mga prinsipyo ngunit maaaring magbigay ng inspirasyon sa iba na magpatibay ng mga katulad na programa sa pamamagitan ng pagpapakita ng isang patunay.

3. **Maglathala ng roadmap ng memory-safety.** Maaaring gumawa ng mga hakbang ang mga tagagawa upang maalis ang isa sa pinakamalaking uri ng kahinaan sa pamamagitan ng paglipat ng mga umiiral nang produkto at pagbuo ng mga bagong produkto gamit ang memory safe languages. Bagama't hindi ito posible sa lahat ng kaso, maaaring isaalang-alang ng mga tagagawa ang pagbuo ng mga wrapper ng application sa memory safe languages sa halip na muling isulat ang buong mga aplikasyon. Maaari rin itong isama kung paano ina-update ng mga tagagawa ang pagkuha, pagsasanay, pagsusuri ng code, at iba pang mga panloob na proseso, pati na rin ang mga paraan kung paano nila tinutulungan ang open source na komunidad na gawin din ito.

4. **I-lathala ang mga resulta.** Habang ina-update ang kanilang SDLC para magkaroon ng secure by design na pilosopiya, makakahanap ang mga organisasyon ng mabilisang panalo, mas maraming panalo na masinsinang mapagkukunan, at ilang hindi inaasahang pag-urong. Sa pamamagitan ng pagpapakita ng kanilang mga panloob na tagumpay at mga hadlang, ang buong industriya ay maaaring matuto mula sa mga resulta.

PRINSIPYO 3: Nangunguna mula sa Itaas

PALIWANAG

Habang ang pangkalahatang pilosopiya ay tinatawag na "secure by design," ang mga insentibo para sa kaligtasan ng mamimili ay nagsisimula nang maayos bago ang yugto ng disenyo ng produkto. Nagsisimula ang mga ito sa mga layunin sa negosyo at pahiwatig at tahasang mga layunin at ninanais na mga resulta. Kapag ginawang priyoridad ng negosyo ng matataas na pinuno ang seguridad, lumikha ng mga panloob na insentibo, at nagtaguyod ng buong kultura upang gawing kinakailangan ang secure by design, makakamit nila ang pinakamahusay na mga resulta.

Bagama't mahalaga ang kadalubhasaan sa teknikal na paksa sa seguridad ng produkto, hindi ito isang bagay na maaaring ipaubaya lamang sa mga teknikal na kawani. Ito ay isang prayoridad sa negosyo na dapat magsimula sa tuktok.

Ang ilang mga tao ay nagtaka, kung ang isang tagagawa ng software ay tinatanggap ang unang dalawang prinsipyo at gumagawa ng mga makabuluhang artifact, kailangan pa ba ang ikatlong prinsipyo? Kung paano itinatatag ng isang kumpanya ang kanyang pananaw, misyon, mga halaga, at kultura ay makakaapekto sa produkto, at ang mga elementong iyon ay may mabigat na bahagi sa itaas. Nakikita namin ito sa iba pang mga industriya na gumawa ng mga makabuluhang pagpapabuti sa kaligtasan at kalidad. Ang kilalang dalubhasa sa kalidad na si J.M. Juran ay sumulat:

> ***Ang pagkamit ng kalidad na pamumuno ay nangangailangan na ang mga nakatataas na tagapamahala ay personal na mangasiwa sa pamamahala para sa kalidad. Sa mga kumpanyang nakakuha ng kalidad na pamumuno, personal na ginabayan ng mga nakatataas na tagapamahala ang inisyatiba. Hindi ko alam ang anumang mga pagbubukod. [3]***

Naniniwala kami na ang seguridad ay isang sub-category ng kalidad ng produkto. Kapag ang seguridad at kalidad ay naging mga pangangailangan sa negosyo sa halip na mga teknikal na pag-andar na iniiwan lamang sa mga teknikal na kawani, ang mga organisasyon ay makakatugon sa mga pangangailangan sa seguridad ng kanilang mga mamimili nang mas mabilis at mahusay. Bukod dito, ang pamumuhunan ng mga kinakailangang mapagkukunan upang matiyak na ang seguridad ng software ay isang pangunahing priyoridad sa negosyo mula sa simula ay magbabawas sa mga pangmatagalang gastos sa pagtugon sa mga depekto sa software–at dahil dito, babawasan ang mga panganib sa pambansang seguridad.

Sa parehong paraan kung paano ipinatupad ng mga leadership team ang mga programa ng corporate social responsibility (CSR), lumalaki ang kamalayan na ang mga corporate board, kabilang ang mga tagagawa ng software, ay dapat magkaroon ng mas aktibong papel sa paggabay sa mga programa sa cybersecurity. Minsan ginagamit ang terminong corporate cyber responsibility (CCR) upang ilarawan ang umuusbong na ideyang ito.

PAGPAPAKITA NG PRINSIPYO NA ITO

Upang ipakita ang prinsipyong ito, ang mga tagagawa ng software ay dapat gumawa ng mga hakbang kabilang ang mga sumusunod:

1. **Isama ang mga detalye ng secure by design program sa corporate financial reports.** Kung ang tagagawa ay isang pampublikong kinakalakal na kumpanya, magdagdag ng isang seksyon sa bawat taunang ulat na nakatuon sa mga pagsisikap para sa secure by design. Karaniwan para sa mga taunang ulat sa pananalapi ng sasakyan na magsama ng mga seksyon sa kaligtasan ng nagmamaneho at pasahero, kabilang ang impormasyon tungkol sa sentralisado at ipinamahagi na mga komite sa kalidad at kaligtasan. Ang pagdedetalye ng programang secure by design sa isang ulat sa pananalapi ay magpapakita na ang organisasyon ay nag-uugnay sa seguridad ng mamimili at mga resulta ng pananalapi ng korporasyon at hindi lamang gumagamit ng isang termino sa mga materyales sa marketing dahil ito ay kasalikuyang nauuso.

2. **Magbigay ng mga regular na ulat sa iyong lupon ng mga direktor.** Ang mga ulat ng chief information security officer (CISO) sa mga corporate board ay karaniwang may kasamang impormasyon tungkol sa kasalukuyan at nakaplanong mga programa sa seguridad, mga banta, pinaghihinalaan at nakumpirma na mga insidente sa seguridad, at iba pang mga pagbabago na nakasentro sa postura ng seguridad at kalusugan ng kumpanya. Bilang karagdagan sa pagtanggap ng impormasyon tungkol sa postura ng seguridad ng enterprise, ang mga board ay dapat humiling ng impormasyon tungkol sa seguridad ng produkto at ang epekto nito sa seguridad ng mamimili. Ang mga board ay hindi dapat tumingin lamang sa CISO, ngunit pangunahin sa iba pang mga miyembro ng pamamahala ng kumpanya upang mabawasan ang panganib ng mamimili.

3. **Bigyan ng kapangyarihan ang secure by design executive.** May malaking pagkakaiba sa pagitan ng isang organisasyon kung saan ang mga technical team ay may "executive buy-in," at kung saan ang mga lider ng negosyo ay personal na namamahala sa proseso ng pagpapabuti ng seguridad ng mamimili gamit ang mga karaniwang proseso ng negosyo. Ang terminong "executive buy-in" ay nagpapahiwatig na kailangan ng isang tao na ibenta ang ideya ng isang programa sa kaligtasan ng mamimili sa halip na ito ay isang nangungunang layunin sa negosyo. Dapat bigyan ng kapangyarihan ang executive na ito na maimpluwensyahan ang mga pamumuhunan ng produkto upang makamit ang mga resulta ng seguridad ng mamimili.

4. **Lumikha ng makabuluhang panloob na mga insentibo.** Habang nag-iingat na huwag gumawa ng mga masasamang insentibo, ihanay ang mga sistema ng reward upang mapabuti ang seguridad ng mamimili upang tumugma sa iba pang pinahahalagahang gawi at resulta. Mula sa secure by design executive hanggang sa pamamahala ng produkto, software development, suporta, benta, legal, at iba pang organisasyon, hinabi ang mga insentibo sa seguridad ng mamimili sa pagkuha, promosyon, suweldo, bonus, stock option, at iba pang karaniwang proseso sa pagpapatakbo ng negosyo. Halimbawa, kapag nagtatatag ng pamantayan para sa pag-promote ng mga developer ng software, isama ang mga pagsasaalang-alang para sa pagpapabuti ng seguridad ng produkto kasama ng iba pang pamantayan tulad ng uptime, pagganap, at mga pagpapabuti ng katangian.

5. **Gumawa ng secure by design na konseho.** Sa ilang industriya, karaniwan para sa mga organisasyon na lumikha ng isang sentral na konseho ng kalidad, at mag-embed ng mga de-kalidad na kinatawan sa mga pangunahing dibisyon o unit ng negosyo. Sa pamamagitan ng pagsasama ng parehong sentralisado at distributed na mga miyembro, ang mga pangkat na ito ay nagsusumikap upang mapabuti ang kalidad laban sa pinakamataas na antas ng mga layunin habang tumatanggap ng telemetry mula sa malalim na organisasyon. Katulad nito, ang isang secure by design na konseho ay magpapahusay ng seguridad laban sa secure by design na mga layunin sa buong organisasyon.

6. **Gumawa at magpagtupad ng mga konseho para sa mga mamimili.** Maraming mga tagagawa ng software ang may mga konseho ng mamimili na binubuo ng mga mamimili mula sa iba't ibang rehiyon, industriya, at laki. Ang mga konsehong ito ay maaaring magbigay ng maraming impormasyon tungkol sa mga tagumpay at hamon ng mamimili sa pag-deploy ng mga produkto ng kumpanya. Buuin ang agenda ng konseho na may mga nakatuong paksa na tumutugon sa kaligtasan ng mamimili, kahit na hindi ito kasalukuyang nasa isip ng mga kalahok. Isaalang-alang kung saan nag-uulat ang konseho ng mga mamimili at kung paano i-tap ang mga kalahok para sa mga kaalaman sa seguridad ng produktong nailabas. Halimbawa, may pagkiling ba ang konseho sa mga layunin ng marketing at pagbebenta, o pamamahala ng produkto? Ang secure by design executive ay dapat tumulong na patnubayan ang mga pakikipag-ugnayan ng mamimili na ito at dapat na iugnay ang mga ito sa iba pang elemento sa papel na ito, gaya ng mga field study.

MGA TAKTIKANG SECURE BY DESIGN

Ang Secure Software Development Framework (SSDF), na kilala rin bilang National Institute of Standards and Technology's (NIST's) SP 800-218, ay isang pangunahing hanay ng mataas na antas na ligtas na software development na mga kasanayan na maaaring isama sa bawat yugto ng software development lifecycle (SDLC). Ang pagsunod sa mga kasanayang ito ay makakatulong sa mga producer ng software na maging mas epektibo sa paghahanap at pag-alis ng mga kahinaan sa inilabas na software, pagaanin ang potensyal na epekto ng pagsasamantala sa mga kahinaan, at tugunan ang mga ugat na sanhi ng mga kahinaan upang maiwasan ang mga pag-ulit sa hinaharap.

Hinihikayat ng mga organisasyong may-akda ang paggamit ng mga taktikang secure by design, kabilang ang mga prinsipyong tumutukoy sa mga kasanayan sa SSDF. Ang mga tagagawa ng software ay dapat bumuo ng isang nakasulat na roadmap upang magpatibay ng mas ligtas sa pamamagitan ng disenyo ng mga kasanayan sa pagbuo ng software sa kanilang portfolio. Ang sumusunod ay isang hindi kumpletong paglalarawan ng listahan ng mga pinakamahuhusay na kagawian sa roadmap:

- **Mga programming languages na ligtas sa memorya (SSDF PW.6.1).** Unahin ang paggamit ng mga memory safe na wika hangga't maaari. Kinikilala ng mga organisasyong may-akda na ang mga pagpapagaan na partikular sa memorya ay maaaring maging kapaki-pakinabang na mga taktika sa mas maikling panahon para sa mga legacy na codebase. Kasama sa mga halimbawa ang mga pagpapahusay sa wika ng C/C++, pagpapagaan ng hardware, randomization ng layout ng address space (ASLR), integridad ng control-flow (CFI), at fuzzing. Gayunpaman, mayroong lumalagong pinagkasunduan na ang pag-aampon ng mga memory safe programming language ay maaaring alisin ang klase ng depekto, at ang mga tagagawa ng software ay dapat magsaliksik ng mga paraan upang gamitin ang mga ito. Ang ilang mga halimbawa ng modernong memory safe na mga wika ay kinabibilangan ng C#, Rust, Ruby, Java, Go, at Swift. Basahin ang memory safety ng NSA information sheet para sa higit pa.

- **Ligtas na Pundasyon ng Hardware.** Isama ang mga tampok na arkitektura na nagbibigay-daan sa pinong proteksyon ng memorya, tulad ng mga inilarawan ng Capability Hardware Enhanced RISC Instructions (CHERI) na maaaring mag-extend ng conventional hardware Instruction-Set Architectures (ISA), pati na rin ang iba pang katangian tulad ng Trusted Platform Module at Hardware Security Module. Para sa higit pang impormasyon, bisitahin ang CHERI webpage ng Unibersidad ng Cambridge.

- **Ligtas na Mga Bahagi ng Software (SSDF PW 4.1).** Kumuha at magmentena ng mahusay na ligtas na mga bahagi ng software (hal., mga library ng software, module, middleware, frameworks) mula sa na-verify na komersyal, open source, at iba pang mga third-party na developer upang matiyak ang matatag na seguridad sa mga produkto ng consumer software.

- **Mga framework ng template ng web (SSDF PW.5.1).** Gumamit ng mga framework ng template ng web na nagpapatupad ng awtomatikong pagtakas sa input ng gumagamit upang maiwasan ang mga pag-atake sa web, kagaya ng cross-site scripting.

- **Mga naka-parameter na query (SSDF PW 5.1).** Gumamit ng mga parameterized na query sa halip na isama ang input ng user sa mga query, upang maiwasan ang mga pag-atake ng SQL injection.

- **Static at dynamic na application security testing (SAST/DAST)** (SSDF PW.7.2, PW.8.2). Gamitin ang mga tool na ito para suriin ang source code ng produkto at gawi ng application para makita ang mga kasanayang madaling kapitan ng error. Sinasaklaw ng mga tool na ito ang mga isyu mula sa hindi wastong pamamahala ng memorya hanggang sa pagbuo ng query sa database na madaling kapitan ng error (hal., hindi nakatakas na input ng gumagamit na humahantong sa SQL injection). Ang mga tool ng SAST at DAST ay maaaring isama sa mga proseso ng pag-unlad at awtomatikong tumakbo bilang bahagi ng pagbuo ng software. Ang SAST at DAST ay dapat umakma sa iba pang mga uri ng pagsubok, tulad ng pagsubok sa yunit at pagsubok sa pagsasama, upang matiyak na sumusunod ang mga produkto sa inaasahang mga kinakailangan sa seguridad. Kapag natukoy ang mga isyu, dapat magsagawa ang mga tagagawa ng root-cause analysis upang sistematikong matugunan ang mga kahinaan.

- **Pagsusuri ng code** (SSDF PW.7.1, PW.7.2). Sikaping tiyakin na ang code na isinumite sa mga produkto ay dumadaan sa mga diskarte sa pagkontrol sa kalidad, kagaya ng peer review ng ibang mga developer o "error seeding."
- **Software Bill of Materials (SBOM)** (SSDF PS.3.2, PW.4.1). Isama ang paglikha ng SBOM[4] upang magbigay ng bisibilidad sa hanay ng software na napupunta sa mga produkto.
- **Mga programa sa pagbubunyag ng kahinaan** (SSDF RV.1.3). Magtatag ng mga programa sa pagsisiwalat ng kahinaan na nagpapahintulot sa mga mananaliksik ng seguridad na mag-ulat ng mga kahinaan at makatanggap ng legal na ligtas na daungan sa paggawa nito. Bilang bahagi nito, dapat magtatag ang mga tagapag-tustos ng mga proseso upang matukoy ang mga ugat ng mga natuklasang kahinaan. Dapat kasama sa mga naturang proseso ang pagtukoy kung ang paggamit ng alinman sa secure by design na kasanayan sa dokumentong ito (o iba pang katulad na kasanayan) ay pumigil sa pagpapakilala ng kahinaan.
- **Pagkumpleto ng CVE.** Tiyaking kasama sa mga nalathala na CVE ang root cause o common weakness enumeration (CWE) upang paganahin ang pagsusuri sa buong industriya ng mga bahid sa disenyo ng seguridad ng software. Bagamat ang pagtiyak na ang bawat CVE ay tama at kumpleto ay maaaring mangangailangan ng karagdagang oras, pinapayagan nito ang magkakaibang entity na makita ang mga uso sa industriya na nakikinabangan ng lahat ng mga tagagawa at mamimili. Para sa higit pang impormasyon sa pamamahala sa mga kahinaan, tingnan ang patnubay ng CISA na Tukoy sa Pagkakategorya ng Stakeholder-Specific Vulnerability (SSVC).
- **Defense-in-Depth.** Idisenyo ang imprastraktura upang ang kompromiso ng isang kontrol sa seguridad ay hindi magresulta sa kompromiso ng buong sistema. Halimbawa, ang pagtiyak na ang mga pribilehiyo ng user ay makitid na nakalaan, at ang mga listahan ng kontrol sa paggamit ay ginagamit maaaring mabawasan ang epekto ng isang nakompromisong account. Gayundin, ang mga diskarte sa sandboxing ng software ay maaaring mag-kwarantina ng isang kahinaan upang limitahan ang kompromiso ng isang buong aplikasyon.
- **Satisfy Cybersecurity Performance Goals (CPGs).** Magdisenyo ng mga produkto na nakakatugon sa mga pangunahing kasanayan sa seguridad. Binabalangkas ng Mga Layunin sa Pagganap ng Seguridad sa Cyber ng CISA ang pangunahing, baseline na mga hakbang sa seguridad sa cyber na dapat ipatupad ng mga organisasyon. Bukod pa rito, para sa higit pang mga paraan upang palakasin ang postura ng iyong organisasyon, tingnan ang Cyber Assessment Framework ng UK na may pagkakatulad sa mga CPG ng CISA. Kung nabigo ang isang tagagawa na matugunan ang mga CPG— gaya ng hindi nangangailangan ng phishing-resistant na MFA para sa lahat ng empleyado— kung gayon hindi sila makikitang naghahatid ng secure by design na mga produkto.

Kinikilala ng mga organisasyong may-akda na ang mga pagbabagong ito ay makabuluhang pagbabago sa postura ng isang organisasyon. Dahil dito, dapat bigyang-priyoridad ang kanilang pagpapakilala batay sa iniangkop na pagmomodelo ng pagbabanta, pagiging kritikal, pagiging kumplikado, at epekto sa negosyo. Maaaring ipakilala ang mga kasanayang ito para sa bagong software at unti-unting pinalawak upang masakop ang mga karagdagang kaso at produkto ng paggamit. Sa ilang mga kaso, ang pagiging kritikal at panganib na postura ng isang partikular na produkto ay maaaring makakuha ng isang pinabilis na iskedyul upang gamitin ang mga kasanayang ito. Sa iba pa, ang mga kasanayan ay maaaring ipasok sa isang legacy na codebase at ipatupad sa darating na panahon.

[4] Ang ilan sa mga organisasyong may-akda ay nagsisiyasat ng mga alternatibong pamamaraan sa pagkakaroon ng mga kasiguruhan sa seguridad sa paligid ng software supply chain.

MGA TAKTIKANG SECURE BY DEFAULT

Bilang karagdagan sa paggamit ng secure by design na mga kasanayan sa pagbuo, inirerekomenda ng mga organisasyong may-akda ang mga tagagawa ng software na unahin ang secure by default na mga pagsasaayos sa kanilang mga produkto. Dapat itong magsikap na i-update ang mga produkto upang umayon sa mga kagawiang ito habang nire-refresh ang mga ito. Halimbawa:

- **Alisin ang mga default na password.** Ang mga produkto ay hindi dapat may kasama na mga default na password na ibinabahagi sa pangkalahatan. Upang alisin ang mga default na password, inirerekomenda ng mga organisasyong may-akda ang mga produkto na kailangan ng mga administrator na magtakda ng malakas na password sa panahon ng pag-install at pagsasaayos o para ipadala ang produkto na may natatangi at malakas na password para sa bawat aparato.

- **Ipag-utos ang multifactor authentication (MFA) para sa mga may pribilehiyong gumagamit.** Napansin namin na maraming deployment ng enterprise ang pinamamahalaan ng mga administrator na hindi nagpoprotekta sa kanilang mga account gamit ang MFA. Dahil ang mga administrador ay high-value na mga target, ang mga produkto ay dapat gumawa ng MFA opt-out sa halip na mag-opt-in. Dagdag pa, dapat na regular na paalalahanan ng sistema ang administrador na gamitin ang MFA hanggang sa matagumpay nilang paganahin ito sa kanilang account. Ang NCSC ng Netherlands ay may patnubay na katumbas ng CISA, bisitahin ang kanilang Mature Authentication Factsheet para sa higit pang impormasyon.

- **Single sign-on (SSO).** Ang mga IT application ay dapat magpatupad ng single sign on support sa pamamagitan ng mga modernong bukas na pamantayan. Kasama sa mga halimbawa ang Security Assertion Markup Language (SAML) o OpenID Connect (OIDC.) Ang kakayahang ito ay dapat gawing available bilang default nang walang karagdagang gastos.

- **Secure na Pag-log.** Magbigay ng mataas na kalidad na mga audit log sa mga mamimili nang walang dagdag na bayad o karagdagang pagsasaayos. Ang mga audit log ay mahalaga para sa pag-detekto at pagpapalaki ng mga potensyal na insidente sa seguridad. Mahalaga rin ang mga ito sa panahon ng pagsisiyasat ng pinaghihinalaang o nakumpirmang insidente sa seguridad. Isaalang-alang ang pinakamahuhusay na kagawian gaya ng pagbibigay ng madaling pakikisama sa mga security information at event management na sistema na may access sa application programming interface (API) na gumagamit ng coordinated universal time (UTC), standard time zone formatting, at mahusay na mga pamamaraan sa dokumentasyon.

- **Profile sa Pagpapahintulot ng Software.** Ang mga supplier ng software ay dapat magbigay ng mga rekomendasyon sa mga awtorisadong tungkulin sa profile at sa kanilang itinalagang kaso ng paggamit. Dapat magsama ang mga tagagawa ng nakikitang babala na nag-aabiso sa mga mamimili ng mas mataas na panganib kung lumihis sila mula sa inirerekomendang pahintulot sa profile. Halimbawa, maaaring tingnan ng mga medikal na doktor ang lahat ng mga rekord ng pasyente, ngunit ang isang medikal na scheduler ay may limitadong paggamit sa ilang partikular na impormasyon na kinakailangan para sa pag-iskedyul ng mga appointment.

- **Seguridad na naghahanap ng pasulong sa pagiging tugmang palikod.** Madalas, ang mga katangian na backwards-compatible legacy ay kasama, at kadalasang pinapagana, sa mga produkto sa kabila ng idinudulot na mga panganib sa seguridad ng produkto. Unahin ang seguridad kaysa sa backwards compatibility, na nagbibigay ng kapangyarihan sa mga security team na alisin ang mga hindi ligtas na katangian kahit na nangangahulugan ito na magdulot ng mga paglabag sa pagbabago.

- **Subaybayan at bawasan ang laki ng "hardening guide."** Bawasan ang laki ng "hardening guides" na kasama sa mga produkto at sikaping matiyak na lumiliit ang laki sa paglipas ng panahon habang inilalabas ang mga bagong bersyon ng software. Isama ang mga bahagi ng "hardening guide" bilang default na pagsasaayos ng produkto. Kinikilala ng mga organisasyong may-akda na ang mga pinaikling gabay sa pagpapatigas ay nagreresulta mula sa patuloy na pakikipagsosyo sa mga kasalukuyang mamimili at kasama ang mga pagsisikap ng maraming pangkat na gumagawa sa produkto, kabilang ang karanasan ng gumagamit (UX).

- **Isaalang-alang ang mga kahihinatnan ng karanasan ng gumamit ng mga setting ng seguridad.** Ang bawat bagong setting ay nagdaragdag sa pasanin ng mga huling gagamit at dapat masuri kasabay ng benepisyo ng negosyo na nakukuha nito. Ang pinakamaganda, wala sanang setting; sa halip, ang pinakaligtas na setting ay dapat isama sa produkto bilang default. Kapag kailangang isaayos, ang default na opsyon ay dapat na malawakang ligtas laban sa mga karaniwang banta.

Kinikilala ng mga organisasyong may-akda ang mga pagbabagong ito ay maaaring may mga epekto sa pagpapatakbo sa kung paano ginagamit ang software. Kaya, napakamahalaga ang puna ng mamimili sa pagbabalanse ng mga pagsasaalang-alang sa pagpapatakbo at seguridad. Naniniwala kami na ang pagbuo ng mga nakasulat na roadmap at suporta sa executive na nagbibigay-priyoridad sa mga ideyang ito sa pinakamahalagang produkto ng isang organisasyon ang unang hakbang sa paglipat patungo sa mga ligtas na kasanayan sa pagbuo ng software. Bagama't mahalaga ang input ng mamimili, naobserbahan namin ang mahahalagang kaso kung saan ayaw o hindi nagawa ng mga mamimili na magpatibay ng mga pinahusay na pamantayan, kadalasan ay mga network protocol. Mahalaga para sa mga tagagawa na lumikha ng makabuluhang mga insentibo para sa mga mamimili na manatiling napapanahon at huwag payagan silang manatiling mahina nang walang katiyakan.

MGA GABAY SA HARDENING LABAN SA LOOSENING

Ang mga hardening guide ay maaaring magresulta mula sa kakulangan ng mga kontrol sa seguridad ng produkto na nakapaloob sa arkitektura ng isang produkto mula sa simula ng pagbuo. Dahil dito, ang mga hardening guide ay maaari ding maging roadmap para sa mga kalaban upang matukoy at mapagsamantalahan ang mga hindi ligtas na katangian. Karaniwan para sa maraming organisasyon na walang kamalayan sa mga hardening guide, kaya iniiwan nila ang kanilang mga setting ng pagsasaayos ng kagamitan sa isang hindi ligtas na katayuan. Ang baligtad na modelo na kilala bilang isang loosening guide ang dapat ipalit sa mga naturang hardening guide at ipaliwanag kung alin sa mga pagbabago ang dapat gawin ng mga gumagamit habang naglilista rin ng mga mapanganib na resulta sa seguridad. Ang mga gabay na ito ay dapat isulat ng mga security practitioner na maaaring ipaliwanag ang mga tradeoff sa malinaw na wika upang madagdagan ang pagkakataong mailapat ang mga ito nang tama.

Sa halip na bumuo ng mga hardening guide na naglilista ng mga paraan para sa pag-secure ng mga produkto, inirerekomenda ng mga organisasyong may-akda sa mga tagagawa ng software na lumipat sa isang secure by default na pamaraan at nagbibigay ng mga "loosening guide." Ipinapaliwanag ng mga gabay na ito ang panganib sa negosyo ng mga desisyon sa simple, nauunawaan na wika, at maaaring magpataas ng kamalayan ng organisasyon sa mga panganib sa malisyosong cyber intrusions. Ang mga tradeoff sa seguridad ay dapat matukoy ng mga senior executive ng mga mamimili, na binabalanse ang seguridad sa iba pang mga kinakailangan sa negosyo.

MGA REKOMENDASYON PARA SA MGA KUSTOMER

Inirerekomenda ng mga organisasyong may-akda sa mga organisasyon na panagutin ang kanilang mga tagagawa ng software para sa mga resulta ng seguridad ng kanilang mga produkto. Bilang bahagi nito, inirerekomenda ng mga organisasyong may-akda sa mga executive na unahin ang kahalagahan ng pagbili ng secure by design at secure by default na mga produkto. Maaari itong mahayag sa pamamagitan ng pagtatatag ng mga patakaran na nangangailangan na tasahin ng mga departamento ng IT ang seguridad ng software bago ito bilhin, pati na rin ang pagbibigay ng kapangyarihan sa mga departamento ng IT na itulak pabalik kung kinakailangan. Dapat bigyan ng kapangyarihan ang mga kagawaran ng IT na bumuo ng pamantayan sa pagbili na nagbibigay-diin sa kahalagahan ng secure by design at secure by default na mga kasanayan (kapwa yaong nakabalangkas sa dokumentong ito at iba pang binuo ng organisasyon). Higit pa rito, ang mga kagawaran ng IT ay dapat na suportahan ng executive management kapag ipinapatupad ang mga pamantayang ito sa mga desisyon sa pagbili. Ang mga desisyon ng organisasyon na tanggapin ang mga panganib na nauugnay sa mga partikular na produkto ng teknolohiya ay dapat na pormal na idokumento, aprubahan ng isang senior executive ng negosyo, at regular na iharap sa lupon ng mga direktor.

Ang mga pangunahing serbisyo sa IT ng enterprise na sumusuporta sa postura ng seguridad ng organisasyon, tulad ng network ng enterprise, pagkakakilanlan ng enterprise at pamamahala ng pag-access, at mga pagpapatakbo ng seguridad at mga kakayahan sa pagtugon, ay dapat makita bilang mga kritikal na function ng negosyo na pinondohan upang iayon sa kanilang kahalagahan sa tagumpay ng misyon ng organisasyon. Ang mga organisasyon ay dapat bumuo ng plano upang itaas ang mga kakayahan na ito upang magamit ang mga tagagawa na sumasaklaw sa secure by design at secure by default na mga kasanayan.

Kung saan posible, dapat magsikap ang mga organisasyon na bumuo ng mga madiskarteng relasyon sa kanilang mga pangunahing tagapagtustos ng IT. Kasama sa mga naturang relasyon ang pagtitiwala sa maraming antas ng organisasyon at nagbibigay ng mga paraan upang lutasin ang mga isyu at tukuyin ang mga ibinahaging priyoridad. Ang seguridad ay dapat na isang kritikal na elemento ng naturang mga relasyon at dapat na magsikap ang mga organisasyon na palakasin ang kahalagahan ng secure by design at secure by default na mga kasanayan sa parehong pormal (hal., mga kontrata o kasunduan sa vendor) at impormal na mga parte ng relasyon. Dapat asahan ng mga organisasyon ang katapatan mula sa kanilang mga tagapagtustos ng teknolohiya tungkol sa kanilang internal control posture pati na rin ang kanilang roadmap patungo sa pagpapatibay ng mga secure by design at secure by default na mga kasanayan.

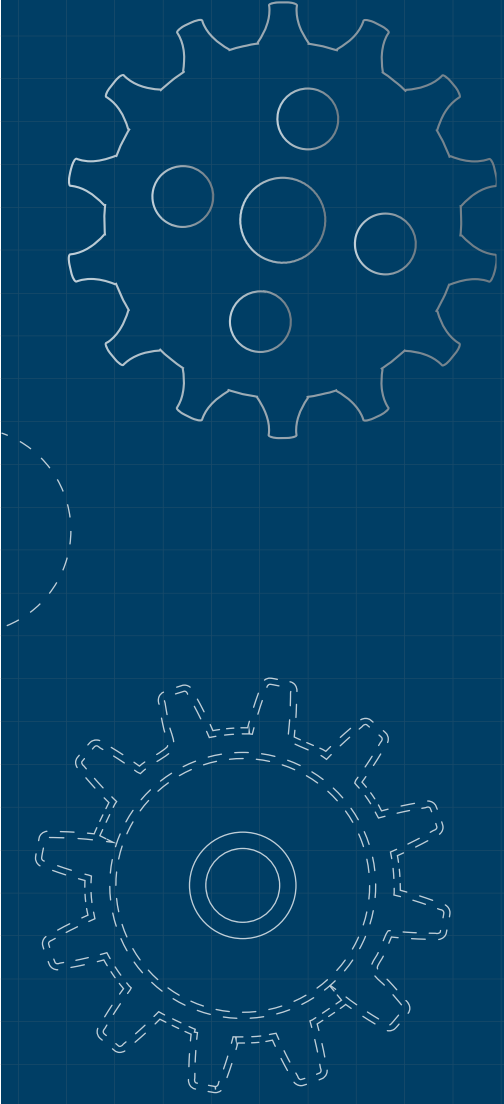
Bilang karagdagan sa paggawa ng secure by default na isang priyoridad sa loob ng isang organisasyon, dapat makipagtulungan ang mga lider ng IT sa kanilang mga kapantay sa industriya upang maunawaan kung aling mga produkto at serbisyo ang pinakamahusay na naglalaman ng mga prinsipyong ito sa disenyo. Dapat may koordinasyon ng mga pinunong ito sa kanilang mga kahilingan upang matulungan ang mga tagagawa na bigyang-priyoridad ang kanilang paparating na mga hakbangin sa seguridad. Sa pamamagitan ng pagtutulungan, makakatulong ang mga mamimili na magbigay ng makabuluhang input sa mga tagagawa at lumikha ng mga insentibo para unahin nila ang seguridad.

Kapag gumagamit ng mga cloud system, dapat tiyakin ng mga organisasyon na nauunawaan nila ang modelo ng magkabahagi sa responsibilidad sa kanilang tagapagtustos ng teknolohiya. Ibig sabihin, ang mga organisasyon ay dapat magkaroon ng kalinawan sa mga responsibilidad sa seguridad ng tagapagtustos at hindi lamang ang mga responsibilidad ng mga mamimili.

Dapat bigyang-priyoridad ng mga organisasyon ang mga cloud provider na malinaw tungkol sa kanilang katayuan sa seguridad, mga panloob na kontrol, at kakayahang tuparin ang kanilang mga obligasyon sa ilalim ng modelo ng magkabahagi sa responsibilidad.

PAGTATATWA

Ang impormasyon sa ulat na ito ay ibinibigay “as is” para sa mga layuning pang-impormasyon lamang. Ang CISA at ang mga organisasyong may-akda ay hindi nag-eendorso ng anumang komersyal na produkto o serbisyo, kabilang ang anumang mga paksa ng pagsusuri. Anumang pagtukoy sa mga partikular na komersyal na entity o komersyal na produkto, proseso, o serbisyo sa pamamagitan ng marka ng serbisyo, trademark, tagagawa, o kung hindi man ay hindi bumubuo o nagpapahiwatig ng pagsang-ayon-, rekomendasyon, o paboritismo ng CISA at ng mga organisasyong may-akda. Ang dokumentong ito ay isang pinagsamang inisyatiba ng CISA na hindi awtomatikong nagsisilbing isang dokumento ng regulasyon.



Mga mapagkukunan

CISA

- Gabay sa SBOM ng CISA
- Ang mga Cross-Sector na Layunin sa Pagganap sa Seguridad sa Cyber ng CISA
- Mga Patnubay sa Technology Interoperability
- Pagtatanggol ng CISA at NIST Laban sa Mga Pag-atake sa Supply Chain ng Software
- Ang Halaga ng Hindi Ligtas na Teknolohiya at Ano ang Magagawa Natin Tungkol Dito | CISA
- Ihinto ang Pagpasa ng Buck sa Seguridad sa Cyber: Bakit Dapat Bumuo ang Mga Kumpanya ng Kaligtasan sa Mga Tech na Produkto (foreignaffairs.com)
- Gabay sa Stakeholder-Specific Vulnerability Categorization (SSVC) ng CISA
- Phishing Resistant MFA Fact Sheet ng CISA
- Gabay sa Cyber para sa Maliit na Negosyo | CISA

NSA

- Ang Seguridad sa Cyber Information Sheet sa Memory Safety ng NSA
- Ang ESF ng NSA ay Nagse-secure ng Software Supply Chain: Pinakamahuhusay na Kasanayan para sa Mga Supplier

FBI

- Pag-unawa at Pagtugon sa SolarWinds Supply Chain Attack: Ang Pananaw ng Pederal
- Ang Pagbabantang Cyber - Tugon at Pag-uulat
- Stratehiya ng Cyber ng FBI

Pambansang Institusyon ng Mga Pamantayan at Teknolohiya (NIST)

- Mga Alituntunin sa Pagkikilanlang Digital ng NIST
- Balangkas sa Seguridad sa Cyber ng NIST
- Balangkas sa Ligtas na Software Development (SSDF) ng NIST

Sentro ng Seguridad sa Cyber ng Australia (ACSC)

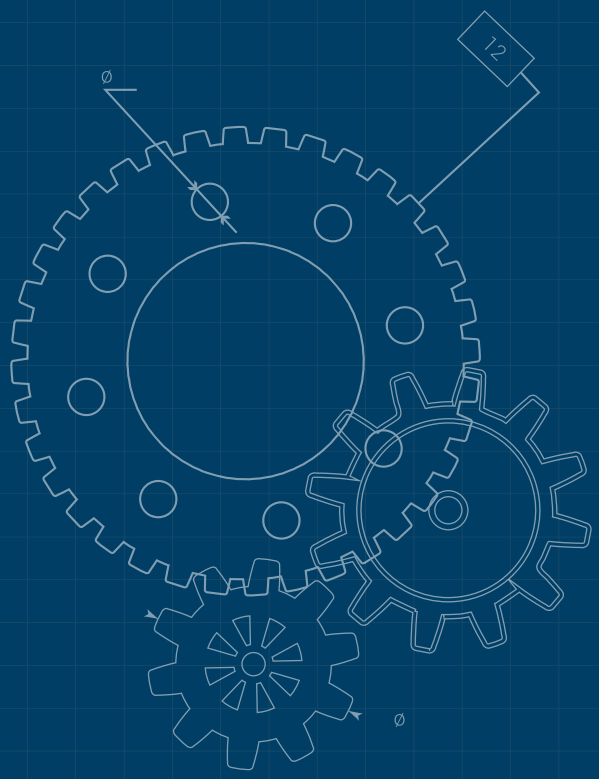
- Ang IoT Code of Practice Guidance ng ACSC para sa mga Tagagawa

Ang Pambansang Sentro ng Seguridad sa Cyber ng United Kingdom (UK)

- Ang Cyber Assessment Framework ng UK
- Gabay sa Secure Development at Deployment ng UK NCSC
- Patnubay ng Vulnerability Management ng UK NCSC
- Vulnerability Disclosure Toolkit ng UK NCSC
- CHERI ng Unibersidad ng Cambridge
- Paalam at salamat sa lahat na mga bahagi - NCSC.GOV.UK

Sentro ng Seguridad sa Cyber ng Canada (CCCS)

- Gabay ng CCCS sa Pagprotekta Laban sa Mga Pag-atake sa Supply Chain ng Software
- Cyber supply chain: Isang diskarte sa pagtatasa ng mga panganib
- Gabay sa CONTI ransomware ng Sentro ng Seguridad sa Cyber ng Canada



Pampederal na Opisina ng Seguridad sa Impormasyon (BSI) ng Germany

- Ang BSI Grundschutz compendium (module CON.8)
- Ang internasyonal na pamantayang IEC 62443, bahagi 4-1
- Ulat ng estado ng seguridad sa IT sa Germany, 2022
- Mga kasanayan sa BSI ng seguridad ng web application

Pambansang Sentry ng Seguridad sa Cyber ng Netherland

- Mature Authentication Factsheet ng NCSC-NL

Pambansang Sentry ng Incident Readiness at Stratehiya sa Cybersecurity (NISC) ng Japan

- Pambansang Stratehiya ng Seguridad sa Cyber ng Japan

Kagawaran ng Ekonomiya, Kalakalan at Industriya (METI) ng Japan

- Gabay sa Pagpapakilala ng Software Bill of Materials (SBOM) para sa Software Management
- Koleksyon ng Mga Halimbawa ng Use Case Tungkol sa Pamamaraan ng Pamamahala para sa Paggamit ng OSS at Pagtiyak ng Seguridad Nito

Ahensya ng Seguridad sa Cyber ng Singapore

- Teknikal na Pagpapayo sa Ligtas na API Development
- Patakaran sa Pagbubunyag ng kahinaan ng CSA SingCERT
- Tugon sa Insidente na Checklist ng CSA SingCERT
- Tugon sa Insidente na Playbook ng CSA SingCERT
- Security by Design na Balangkas ng CSA
- Security by Design Framework Checklist ng CSA
- Ang Gabay ng CSA sa Cyber Threat Modelling
- CSA Cybersecurity Labelling Scheme

Iba pa

- Paano Nabigo Ang Mga Kumplikadong Sistema
- Ang Bagong Hitsura sa kumplikadong pagkabigo ng sistema

MGA SANGGUNIAN

[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.