TLP:CLEAR

Pagbabago sa Balanse ng Panganib sa Cybersecurity: Mga Prinsipyo at Pamamaraan para sa Security-by-Design at -Default

Inilathala: April 13, 2023

Cybersecurity and Infrastructure Security Agency

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

Pagtatatwa: Ang dokumentong ito ay may markang TLP:CLEAR. Ang pagsisiwalat ay hindi limitado. Maaaring gamitin ang TLP:CLEAR kapag ang impormasyon ay may minimal o walang nakikinitang panganib ng maling paggamit, alinsunod sa mga naaangkop na panuntunan at pamamaraan para sa pampublikong pagpapalabas. Alinsunod sa karaniwang mga panuntunan sa copyright, ang TLP:CLEAR na impormasyon ay maaaring ipamahagi nang walang paghihigpit. Para sa karagdagang impormasyon sa Traffic Light Protocol, tingnan ang http://www.cisa.gov/tlp/.

Talaan ng mga 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. Bilang isang halimbawa lamang, ang mga cyber breaches ay nagresulta sa pagkansela ng mga ospital sa mga operasyon at paglilipat ng pangangalaga sa pasyente sa ibang parte ng mundo. Ang hindi ligtas na teknolohiya at mga kahinaan sa mga kritikal na sistema ay maaaring mag-imbita ng mga nakakahamak na pag atake sa cyber, na humahantong sa mga seryosong potensyal na panganib sa kaligtasan[1].

Ngayon higit kailanman, napakahalaga para sa mga tagagawa ng teknolohiya na gawing Secure-by-Design at Secure-by-Default ang mga pokus ng disenyo ng produkto at mga proseso ng pagbuo. Ang ilang mga vendor 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 pumipigil sa mga mamimili na patuloy na magsagawa ng pagsubaybay, regular na pag-update, at kontrol sa pinsala sa kanilang mga sistema upang mabawasan ang mga cyber intrusions. 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 mahihinto natin ang paulit-ulit na paglikha at paglalapat ng mga solusyon.

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 magpasok ng mga hindi ligtas na produkto sa merkado.

[1] Kinikilala ng mga ahensyang 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 na cyber.

Upang magkaroon ng kinabukasan kung saan ang teknolohiya at mga nauugnay na produkto ay mas ligtas para sa mga mamimili , hinihimok ng mga ahensyang 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 . Ang mga produktong Secure-by-Design ay yaong kung saan ang seguridad ng mga mamimili ay isang 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 produktong Secure-by-Default ay yaong mga ligtas na gamitin “out of the box” na may kaunti o walang kinakailangang pagbabago sa ayos at may magagamit na mga katangian sa seguridad na walang karagdagang gastos. Inililipat ng dalawang prinsipyong ito sa mga tagagawa ang 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 teknolohiya 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)
- Computer Emergency Response Team New Zealand (CERT NZ) at Pambansang Sentro ng Cyber Security ng New Zealand (NCSC-NZ).

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 may-akdang ahensya 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

[2] Mula dito ay tinutukoy bilang "mga ahensyang may-akda."

CISA, The Cost of Unsafe Technology and What We Can Do About It.

Secure-by-Design

Ang ibig sabihin ng "Secure-by-Design" ay ang mga produkto ng teknolohiya ay binuo sa paraang sapat na nagpoprotekta laban sa mga nakakahamak na cyber actor na matagumpay na maka-access sa mga device, datos, at konektadong imprastraktura. Ang mga tagagawa ng software ay dapat magsagawa ng pagtatasa ng panganib upang matukoy at matala 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 banta sa cyber.

Inirerekomenda din ang mga kasanayan sa pagpapaunlad ng ligtas na information technology (IT) at maraming patong ng depensa — na kilala bilang defense-in-depth — para maiwasan ang aktibidad sa alanganing sistema o makakuha ng hindi awtorisadong pag-access sa mga sensitibong datos. Inirerekomenda ng mga ahensyang may-akda sa mga tagagawa na gumamit ng isang iniangkop na threat model sa development stage ng produkto upang tugunan ang lahat ng potensyal na banta sa isang sistema at isaalang-alang ang proseso ng pagtalaga sa bawat sistema.

Hinihimok ng mga may-akdang ahensya ang mga tagagawa na magkakaroon ng panglahatang diskarte sa seguridad para sa kanilang mga produkto at plataporma. Ang paglikha ng Secure-by-Design ay nangangailangan ng mga malaking mapagkukunan mula sa mga tagagawa ng software sa bawat yugto sa pagdisenyo ng produkto at proseso ng pagbuo, at hindi dapat ma “bolted on” sa huli. Nangangailangan ito ng matibay na pamumuno ng mga pangunahing pinuno sa negosyo ng tagagawa para gawing priyoridad sa negosyo ang seguridad, hindi lamang bilang isang teknikal na katangian. Ang pakikipagtulungang ito sa pagitan ng mga pinuno ng negosyo at mga teknikal na koponan ay nagsisimula sa umpisa ng pag disenyo at pag-develop, hanggang sa pag-deploy sa mga mamimili at maintenance. Hinihikayat ang mga tagagawa na gumawa ng mahirap na mga tradeoff at investment, kabilang na yung hindi nakikita ng mga mamimili, katulad ng paglipat sa mga programming language na nag-aalis ng malawakang mga 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 posibilidad ng banta.

Walang isang solusyon upang wakasan ang patuloy na banta ng mga malisyosong cyber actor na nagsasamantala sa mga kahinaan sa teknolohiya, at ang mga produktong "Secure-by-Design" ay patuloy na magdaranas ng mga kahinaan; gayunpaman, ang pinagmulan sa maraming kahinaan ay dahil sa isang maliit na subset ng mga pinagmulang kadahilanan. Dapat bumuo ang mga tagagawa ng roadmap upang ihanay ang kanilang mga kasalukuyang produkto sa mga kasanayan sa Secure-by-Design, at tiyaking lilihis lamang sa mga pambihirang sitwasyon.

Tinatanggap ng mga ahensyang may-akda na ang pagtanggap ng responsibilidad sa mga resulta ng

seguridad para sa mga mamimili at pagtiyak sa antas ng seguridad ng mamimiling ito ay maaaring magpataas ng mga gastos sa paggawa. Gayunpaman, ang pagpuhunan sa mga gawi ng "Secure-by-Design" habang gumagawa ng mga bagong produkto ng teknolohiya at pinapanatili ang mga kasalukuyang produkto ay lubos na magpapabuti sa seguridad ng mga mamimili at mabawasan ang posibilidad na malagay sa alanganin. Ang mga prinsipyo ng Secure-by-Design ay hindi lamang nagpapatibay sa seguridad ng mga mamimili at reputasyon ng brand sa mga tagapaglikha, mababawasan din sa kalaunan ang mga gastos sa pagmementena at pag-patch para sa mga tagagawa.

Ang seksyong Mga Rekomendasyon para sa Mga Tagagawa ng Software na nakalista sa ibaba ay nagbibigay ng listahan ng mga inirerekomendang 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 banta “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 ligtas na pagsasaayaos 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 postura ng cybersecurity. Sa pamamagitan ng pag-optimize ng matatag na konpigurasyon 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 upang ipatupad 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 customer sa pamamagitan ng mga prinsipyong Secure-by-Design at -Default.

MGA PRINSIPYO SA SEGURIDAD NG PRODUKTO NG SOFTWARE

Hinihikayat ang mga tagagawa ng teknolohiya na magpatupad ng stratehiya 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. Ang pasanin ng seguridad ay hindi dapat ipasa lamang sa mamimili. Dapat akuin ng mga tagagawa ng software ang mga resulta ng seguridad ng produktong binili ng mamimili at baguhin ang kanilang mga produkto nang naaayon.
2. Tanggapin ang radikal na katapatan at pananagutan. Dapat ipagmalaki ng mga manufacturer ng software ang kanilang sarili sa paghahatid ng mga ligtas at secure 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 advisory sa kahinaan at nauugnay na mga talaan ng mga karaniwang kahinaan at exposure (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. Bumuo 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. Ang pangako sa antas ng executive para sa mga tagagawa ng software na unahin ang seguridad bilang isang kritikal na elemento ng pagbuo ng produkto ay nangangailangan ng pakikipagsama sa mga mamimili ng isang organisasyon upang maunawaan ang:

a. Pagabay sa senaryo ng deployment ng produkto kasama ang iniangkop na modelo ng

pagbabanta

b. Iminungkahing pagpapatupad para sa mga kontrol sa seguridad upang maiayon sa mga prinsipyong Secure-by-Default
c. Pagbibigay ng mga stratehiya ng paglalaan ng resource na iniakma sa laki ng kumpanya at ang kakayahang palitan ang mga lumang pamamaraan sa pagbuo ng mga pamamaraang Secure-by-Design
d. Pangangailangang magpanatili ang bukas na linya ng komunikasyon para sa feedback sa loob at labas (hal., feedback ng empleyado at mamimili) tungkol sa mga isyu sa seguridad ng produkto. Dapat bigyang-diin ang seguridad ng software sa mga internal forum (hal., all-hands o brown bags), pati na rin ang panlabas na marketing ng produkto at pakikipag-ugnayan sa mamimili
e. Mga sukat ng pagiging epektibo sa mga deployment ng mamimili. Gugustuhing malaman ng mga pinakamataas na pinuno sa pagawaan kung saan nakakatulong ang pagpupuhunan sa seguridad na idinisenyo at default sa mga mamimili sa pamamagitan ng pagbaba sa bilis ng mga patch ng seguridad, pagbabawas ng mga pagkakamali sa pag-aayos, at pagpapaliit ng attack surface.

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 pamunuan ng executive 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 bumubuo ng 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 para sa 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 threat model sa panahon ng pagbuo upang unahin ang pinaka kritikal at high-impact na mga produkto. Isinasaalang-alang ng mga threat model 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.

Mga Taktika ng Secure-by-Design

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

Hinihikayat ng mga may-akdang ahensya 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 higit pang Secure-by-Design na mga kasanayan sa pagbuo ng software sa kanilang portfolio. Ang sumusunod ay isang di-kumpletong listahan sa naglalarawang roadmap ng mga pinakamahusay na kasanayan:

- Memory safe programming language (SSDF PW.6.1): Unahin ang paggamit ng mga memory safe na wika hangga't maaari. Kinikilala ng mga ahensyang may-akda na ang iba pang mga pagpapagaan na partikular sa memorya, katulad ng address space layout randomization (ASLR), control-flow integrity (CFI), at fuzzing ay nakakatulong para sa mga lumang codebase, ngunit hindi ito sapat na maituturing na secure-by-design dahil hindi ito sapat para maiwasan ang mga pagbabanta. 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 information sheet ng NSA para sa higit pang impormasyon.
- Secure Hardware Foundation: Isama ang mga tampok na arkitektura na nagbibigay-daan sa fine-grained na proteksyon ng memorya, tulad ng mga inilarawan ng Capability Hardware Enhanced RISC Instructions (CHERI) na maaaring mag-extend ng conventional hardware Instruction-Set Architectures (ISAs). Para sa karagdagang impormasyon, bisitahin ang CHERI webpage ng Unibersidad ng Cambridge.
- Secure Software Components (SSDF PW 4.1): Bilhin at panatilihin ang ligtas na mga bahagi ng software (hal., software library, modules, middleware, frameworks,) mula sa beripikadong komersyal, open source, at iba pang third-party na developer para matiyak ang matatag na seguridad sa mga produktong 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 ng user input upang maiwasan ang mga pag-atake sa web gaya ng cross-site scripting.
- Mga parameterized na query (SSDF PW 5.1): Gumamit ng mga parameterized na query sa halip na isama ang user input sa mga query, upang maiwasan ang mga SQL injection attacks.
- Static at dynamic na pagsubok sa seguridad ng application (SAST/DAST) (SSDF PW.7.2, PW.8.2):

Gamitin ang mga ito para suriin ang source code ng produkto at gawi ng aplikasyon para makita ang mga kasanayang madaling kapitan ng error. Saklaw ng mga tool na ito ang mga isyu gaya ng hindi wastong pamamahala ng memory at sa pagbuo ng query sa database na madaling kapitan ng error (hal., hindi nakatakas na user input na humahantong sa SQL injection). Ang mga gamit ng SAST at DAST ay maaaring isama sa mga proseso ng development at awtomatikong ipatupad bilang bahagi ng development ng software. Ang SAST at DAST ay dapat umakma sa iba pang mga uri ng pagsubok, tulad ng unit testing at integration testing, upang matiyak na sumusunod ang mga produkto sa inaasahang mga kinakailangan sa seguridad. Kapag natukoy ang mga isyu, dapat magsagawa ang mga manufacturer 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 dumaan sa peer review ng ibang mga developer upang matiyak ang mas mataas na kalidad.
- Software Bill of Materials (SBOM) (SSDF PS.3.2, PW.4.1): Isama ang paglikha ng SBOM[3] upang magbigay ng bisibilidad sa hanay ng software na napupunta sa mga produkto.
- Mga programa sa pagsisiwalat ng kahinaan (SSDF RV.1.3): Magtatag ng mga programa sa pagbubunyag 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 tagapanustos 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 mga kasanayang Secure-by-Design sa dokumentong ito (o iba pang katulad na kasanayan) ay maaring pumigil sa pagpasok ng banta.
- Pagkumpleto ng CVE: Tiyakin na ang mga nailathala na CVE ay may kasamang sanhi o karaniwang weakness enumeration (CWE) upang maumpisahan ang pagsusuri sa buong industriya ng mga sanhi ng seguridad ng software. Habang ang pagtiyak na ang bawat CVE ay tama at kumpleto ay maaaring mangailangan ng karagdagang oras, pinapayagan nito ang magkakaibang entity na makita ang mga uso sa industriya na mapapakinabangan ng lahat ng mga manufacturer at mamimili. Para sa higit pang impormasyon sa pamamahala ng mga kahinaan, tingnan ang gabay sa SVCC na partikular sa Stakeholder ng CISA.
- 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 ibinibigay at ang mga listahan ng kontrol sa pag-access ay ginagamit ay maaaring makabawas sa epekto ng isang nakompromisong account. Gayundin, ang mga pamamaraan ng software sandboxing ay maaaring mag-kwarantina ng

[3] Ang ilan sa mga may-akdang mga ahensa ay nagsisiyasat ng mga alternatibong paraan sa pagkakaroon ng mga kasiguruhan sa seguridad ng ugnayan sa panustos ng software.

isang kahinaan upang limitahan ang kompromiso ng isang buong aplikasyon.

- Satisfy Cyber Performance Goals (CPGs): Magdisenyo ng mga produkto na nakakatugon sa mga pangunahing kasanayan sa seguridad. Binabalangkas ng Cybersecurity Performance Goals ng CISA ang pangunahing, baseline na mga hakbang sa cybersecurity na dapat ipatupad ng mga organisasyon. Bukod pa rito, para sa higit pang mga paraan upang palakasin ang postura ng 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— kagaya ng hindi pagpapatupad ng multi-factor na pagpapatunay na lumalaban sa phishing (di-ligal na pangangalap ng impormasyon) para sa lahat ng empleyado— hindi sila maituturing na naghahatid ng mga produktong Secure-by-Design.

Kinikilala ng mga may-akdang ahensya na ang mga pagbabagong ito ay makabuluhang pagbabago sa postura ng isang organisasyon. Dahil dito, dapat unahin ang kanilang pagpapakilala batay sa pagiging kritikal, pagiging kumplikado, at epekto sa negosyo. Maaaring ipakilala ang mga kasanayang ito para sa bagong software at unti-unting ipalawak upang masakop ang mga karagdagang kaso at produkto. Sa ilang mga kaso, ang pagiging kritikal at panganib na postura ng isang partikular na produkto ay maaaring mangailangan ng mas mabilis na iskedyul upang gamitin ang mga kasanayang ito. Sa ibang kaso, ang mga kasanayan ay maaaring ipasok sa isang lumang codebase at isalin sa paglipas ng panahon.

Mga Taktikang Secure-by-Default

Bilang karagdagan sa pagpapatibay ng mga gawi sa pagbuo ng Secure-by-Design, inirerekomenda ng mga ahensyang may-akda sa mga manufacturer ng software na unahin ang mga Secure-by-Default na konpigurasyon sa kanilang mga produkto. Dapat itong magsikap na i-update ang mga produkto upang umayon sa mga kagawiang ito habang pinapasariwa ang mga ito. Halimbawa:

- Tanggalin ang mga default na password: Ang mga produkto ay hindi dapat may kasamang mga default na password na ibinabahagi sa pangkalahatan. Upang alisin ang mga default na password, inirerekomenda ng mga ahensyang may-akda na maglagay ng malakas na password ang mga administrator sa panahon ng pag-install at pagkonpigura sa mga produkto.
    - Mandate Multifactor Authentication (MFA) para sa mga privileged user. 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 administrator 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 administrator 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 na teknolohiya 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 gawin na madaling magamit bilang default nang walang karagdagang gastos.
- Walang Panganib na Pag-log: Magbigay ng mataas na kalidad na mga audit log sa mga mamimili nang walang dagdag na bayad. Ang mga audit log ay mahalaga para sa pagdetekto at pag escalate ng mga potensyal na insidente sa seguridad. Mahalaga rin ang mga ito sa panahon ng pagsisiyasat ng isang pinaghihinalaang o nakumpirmang insidente sa seguridad. Isaalang-alang ang pinakamahuhusay na kagawian gaya ng pagbibigay ng madaling integrasyon sa mga security information at event management (SIEM) 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 ng Awtorisasyon ng Software: Ang mga tagapagtustos ng software ay dapat magbigay ng mga rekomendasyon sa mga awtorisadong profile roles at sa kanilang itinalagang use case. Dapat maglagay ang mga tagagawa ng 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 doktor ang lahat ng mga rekord ng pasyente, ngunit ang isang tagapag-iskedyul ng medikal ay may limitadong access upang matugunan ang impormasyong kinakailangan para sa pag-iskedyul ng mga appointment.
- Forward-looking security sa halip na backwards compatibility: Madalas, ang mga backwards-compatible na lumang feature ay kasama, at kadalasang pinapagana, sa mga produkto kahit na nagdudulot ito ng mga panganib sa seguridad ng produkto. Unahin ang seguridad kaysa sa backwards compatibility, at payagan ang mga pangkat ng seguridad na alisin ang mga hindi matatag na katangian kahit na magdudulot ito ng mga breaking change.
- Subaybayan at bawasan ang laki ng "hardening guide": Bawasan ang laki ng mga "hardening guide" na ginawa para sa mga produkto at sikaping matiyak na lumiliit ito sa paglipas ng panahon habang inilalabas ang mga bagong bersyon ng software. Isama ang mga bahagi ng "hardening guide" bilang default na pagkaayos ng produkto. Kinikilala ng may-akdang mga ahensya na ang mga pinaikling hardening guide ay nagreresulta mula sa patuloy na pakikipagsosyo sa mga kasalukuyang mamimili at mga pagsisikap ng maraming pangkat ng produkto, kabilang ang user experience (UX).
- Isaalang-alang ang mga resulta sa karanasan ng gumagamit sa mga pagkalagay ng seguridad: Ang bawat bagong pagkalagay ay nagpapataas ng imposisyon sa mga gagamit at dapat suriin kasabay ng nakukuhang benepisyo ng negosyo. Kung maaari, hindi dapat umiral ang isang pagkakalagay; sa halip, ang pinakamatatag na pagkakalagay ay dapat isama sa produkto bilang di-nangyari. Kapag kailangan ang pagkaayos, dapat ang opsyon sa seguridad kapag di-nangyari ay mabisa laban sa mga karaniwang banta.

Kinikilala ng may-akdang mga ahensya na ang mga pagbabagong ito ay maaaring magkaroon ng mga epekto sa pagpapatakbo sa kung paano ginagamit ang software. Kaya, kritikal ang input ng mamimili sa pagbabalanse ng mga pagsasaalang-alang sa pagpapatakbo at seguridad. Naniniwala ang mga ahensyang may-akda na ang pagbuo ng mga nakasulat na roadmap at executive support 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 mga puna ng mamimili , nakikita ng mga may-akdang ahensya ang mga kaso kung saan ayaw o hindi ginawa ng mga mamimili ang pinahusay na pamantayan, kadalasan ang mga network protocol. Mahalaga para sa mga tagagawa na lumikha ng makabuluhang mga pagganyak para sa mga mamimili upang mahikayat na manatiling napapanahon at huwag payagang manatiling mahina nang matagal na panahon.

MGA GABAY NG 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 feature. Maraming mga organisasyon ang karaniwang walang kamalayan sa mga hardening guide, kaya iniiwan nila ang kanilang mga setting sa pagkaayos ng kagamitan sa isang hindi ligtas na postura. 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.

Sa halip na bumuo ng mga hardening guide na naglilista ng mga paraan para sa pagka-walang-panganib ng mga produkto, inirerekomenda ng mga ahensyang may-akda sa mga tagagawa ng software na lumipat sa isang Secure-by-Default na paraan sa pamamagitan ng pagbibigay 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 pag-atake sa cyber. Ang mga tradeoff sa seguridad ay dapat matukoy ng mga senior executive ng mga mamimili at binabalanse ang seguridad sa iba pang mga pangangailangan sa negosyo.

MGA REKOMENDASYON PARA SA MGA CUSTOMER

Inirerekomenda ng may-akdang mga ahensya sa mga organisasyon na panagutin ang kanilang mga nagtutustos na tagagawa ng teknolohiya para sa mga resulta ng seguridad ng kanilang mga produkto. Bilang bahagi nito, inirerekomenda ng may-akdang mga ahensya na unahin ng mga executive ng organisasyon ang kahalagahan ng pagbili ng mga Secure-by-Design at Secure-by-Default na mga produkto. Maaari itong gawin sa pamamagitan ng pagtatag ng mga patakaran na nangangailangan na tasahin ng mga departamento ng IT ang seguridad ng software ng tagagawa 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 suportado 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 ng IT ng enterprise na sumusuporta sa postura ng seguridad ng organisasyon, tulad ng enterprise network, enterprise identity at access management, at mga operasyong pangseguridad at mga kakayahan sa pagtugon, ay dapat makita bilang mga kritikal na gawain ng negosyo na pinondohan upang iayon ang kanilang kahalagahan sa tagumpay ng misyon ng organisasyon . Ang mga organisasyon ay dapat bumuo ng plano upang i-upgrade ang mga kakayahan na ito upang magamit ang mga tagagawa na sumasaklaw sa Secure-by-Design at Secure-by-Default na mga kasanayan.

Kung posible, dapat magsikap ang mga organisasyon na bumuo ng mga strategic na 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 transparency 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, ang mga pinuno ng IT ay dapat makipagtulungan 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 i-coordinate ng mga pinunong ito ang 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 shared responsibility sa kanilang supplier 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 postura sa seguridad, mga panloob na kontrol, at kakayahang tuparin ang kanilang mga obligasyon sa ilalim ng modelo ng shared responsibility.

PAGTATATWA

Ang impormasyon sa ulat na ito ay ibinibigay “as is” para sa mga layuning pang-impormasyon lamang. Ang CISA, at ang mga ahensyang 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, at iba pa, ay hindi bumubuo o nagpapahiwatig ng pag-endorso, rekomendasyon, o paboritismo ng CISA at ng may-akdang mga ahensya. Ang dokumentong ito ay isang pinagsamang inisyatiba ng CISA na hindi awtomatikong nagsisilbing isang dokumento ng regulasyon.

MGA MAPAGKUKUNAN

CISA

- Patnubay sa SBOM ng CISA
- Cross-Sector Cybersecurity Performance Goals ng CISA
- Mga Alituntunin 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 Namin Tungkol Dito | CISA
- Itigil ang Pagpasa ng Buck sa Cybersecurity: Bakit Dapat Bumuo ang Mga Kumpanya ng Kaligtasan sa Mga Tech na Produkto (foreignaffairs.com)
- Patnubay ng Stakeholder-Specific Vulnerability Categorization (SSVC) ng CISA
- Mga Phishing Resistant MFA Fact Sheet ng CISA
- Patnubay sa Cyber para sa Maliit na Negosyo | CISA

NSA

- Ang Cybersecurity Information Sheet ng NSA sa Memory Safety
- NSA’s ESF Securing the Software Supply Chain: Pinakamahuhusay na Kasanayan para sa Mga Supplier

FBI

- Pag-unawa at Pagtugon sa SolarWinds Supply Chain Attack: Ang Pananaw na Pampederal
- Ang Cyber Threat - Tugon at Pag-uulat
- Ang Cyber Strategy ng FBI

National Institute of Standards and Technology (NIST)

- Mga Alituntunin sa Digital Identity ng NIST
- Cyber Security Framework ng NIST
- Ang Secure Software Development Framework (SSDF) ng NIST

Ang National Cyber Security Center ng Australya (ACSC)

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

Ang National Cyber Security Center ng United Kingdom

- Ang Cyber Assessment Framework ng UK
- Patnubay sa Secure Development at Deployment ng UK NCSC
- Patnubay sa Pamamahala ng Vulnerability ng UK NCSC
- Toolkit sa Pagbubunyag ng Kahinaan ng UK NCSC
- CHERI ng Unibersidad ng Cambridge
- Paalam at salamat sa lahat ng mga piraso - NCSC.GOV.UK

Ang Cyber Security Center ng Canada (CCS)

- Ang Patnubay ng CCCS sa Pagprotekta Laban sa Mga Pag-atake sa Supply Chain ng Software
- Cyber supply chain: Isang paraan sa pagtatasa ng mga panganib
- Gabay sa ransomware ng CONTI ng Canadian Center for Cyber Security

Federal Office for Information Security (BSI) ng Germany

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

Ang Cyber Security Center ng Netherland

- Ang Mature Authentication Factsheet ng NCSC-NL

Iba pa

- Paano Nabigo ang Mga Kumplikadong Sistema
- Ang Bagong Anyo ng kumplikadong pagkabigo ng sistema