TLP:CLEAR

ການປ່ຽນຄວາມດຸ່ນດ່ຽງຂອງຄວາມສ່ຽງດ້ານຄວາມປອດໄພທາງໄຊເບີ: ຫຼັກການ ແລະ ແນວທາງເພື່ອຄວາມປອດໄພ ໂດຍ-ການອອກແບບ ແລະ - ຄ່າເລີ່ມຕົ້ນ

ພິມເຜີຍແຜ່: ວັນທີ 13 ເມສາ 2023

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

ສາລະບານ

ສາລະບານ 2
ພາບລວມ: ມີຄວາມສ່ຽງໂດຍການອອກແບບ *3*
ຄວາມປອດໄພ-ໂດຍ-ການອອກແບບ Secure-by-Design *5*
ຄວາມປອດໄພ-ໂດຍ-ຄ່າເລີ່ມຕົ້ນ Secure-by-Default *7*
ຄຳແນະນຳສຳລັບຜູ້ຜະລິດຊອບແວ *7*
ຫຼັກການຄວາມປອດໄພຂອງຜະລິດຕະພັນຊອບແວ *8*
ຍຸດທະວິທີການຮັກສາຄວາມປອດໄພໂດຍການອອກແບບ Secure by Design Tactics *10*
ຍຸດທະວິທີການຮັກສາຄວາມປອດໄພໂດຍຄ່າເລີ່ມຕົ້ນ Secure by Default Tactics. *13*
ຄູ່ມືການແຂ່ງຕົວ vs ການຄາຍຕົວ *16*
ຄຳແນະນຳສຳລັບລູກຄ້າ *16*
ຂໍ້ຈຳກັດຄວາມຮັບຜິດຊອບ *18*
ແຫຼ່ງຂໍ້ມູນ *18*

ພາບລວມ: ມີຄວາມສ່ຽງໂດຍການອອກແບບ

ເຕັກໂນໂລຍີຖືກລວມເຂົ້າໃນເກືອບທຸກດ້ານຂອງຊີວິດປະຈຳວັນ.
ລະບົບການຫັນຫນ້າທາງອິນເຕີເນັດແມ່ນເຊື່ອມຕໍ່ກັບລະບົບທີ່ສຳຄັນທີ່ສົ່ງຜົນກະທົບໂດຍກົງຕໍ່ຄວາມຈະເລີນຮຸ່ງເຮືອງທາງດ້ານເສດຖະກິດ, ຊີວິດການເປັນຢູ່ ແລະ ແມ່ນແຕ່ສຸຂະພາບຂອງພວກເຮົາ,
ຕັ້ງແຕ່ການຄຸ້ມຄອງຂໍ້ມູນປະຈຳຕົວສ່ວນບຸກຄົນຈົນເຖິງການຮັກສາທາງການແພດ.
ເປັນພຽງແຕ່ຕົວຢ່າງດຽວເທົ່ານັ້ນ, ການລະເມີດທາງໄຊເບີໄດ້ສົ່ງຜົນໃຫ້ໂຮງໝໍຍົກເລີກການຜ່າຕັດ ແລະ ປ່ຽນທິດທາງການດູແລຄົນເຈັບໃນທົ່ວໂລກ. ເທັກໂນໂລຍີທີ່ບໍ່ປອດໄພ ແລະ
ຊ່ອງໂຫວ່ໃນລະບົບທີ່ສຳຄັນອາດຈະພາໃຫ້ມີການບຸກລຸກທາງໄຊເບີທີ່ເປັນອັນຕະລາຍ,
ເຊິ່ງນຳໄປສູ່ຄວາມສ່ຽງດ້ານຄວາມປອດໄພ[1] ທີ່ຮ້າຍແຮງ.

ໃນປັດຈຸບັນ ມັນເປັນສິ່ງສຳຄັນທີ່ຜູ້ຜະລິດເຕັກໂນໂລຍີຕ້ອງເຮັດໃຫ້ ຄວາມປອດໄພໂດຍການອອກແບບ ແລະ - ຄ່າເລີ່ມຕົ້ນ ເປັນຈຸດທີ່ເນັ້ນຫນັກຂອງຂະບວນການອອກແບບ ແລະ ການພັດທະນາຜະລິດຕະພັນ.
ຜູ້ຂາຍບາງຄົນມີຄວາມກ້າວຫນ້າຢ່າງໃຫຍ່ຫຼວງທີ່ຂັບເຄື່ອນອຸດສາຫະກຳໄປຂ້າງຫນ້າໃນດ້ານການຮັບປະກັນຊອບແວ ໃນຂະນະທີ່ຄົນອື່ນລ້າຫຼັງ.
ຫນ່ວຍງານຜູ້ຂຽນຂໍຊຸກຍູ້ໃຫ້ຜູ້ຜະລິດເຕັກໂນໂລຍີທຸກຄົນສ້າງຜະລິດຕະພັນຂອງຕົນເອງໃນລັກສະນະທີ່ປ້ອງກັນລູກຄ້າຈາກການກວດສອບຢ່າງຕໍ່ເນື່ອງ, ປັບປຸງເປັນປົກກະຕິ ແລະ
ການຄວບຄຸມຄວາມເສຍຫາຍໃນລະບົບຂອງຕົນ ເພື່ອຫຼຸດຜ່ອນການບຸກລຸກທາງໄຊເບີ.
ຜູ້ຜະລິດໄດ້ຮັບການສະຫນັບສະຫນູນໃຫ້ເປັນເຈົ້າຂອງໃນການປັບປຸງຜົນຮັບດ້ານຄວາມປອດໄພຂອງລູກຄ້າຂອງພວກເຂົາ. ໃນອາດີດ,
ຜູ້ຜະລິດເຕັກໂນໂລຍີໄດ້ເພິ່ງພາການແກ້ໄຂຈຸດອ່ອນທີ່ພົບເຫັນຫຼັງຈາກລູກຄ້າປັບໃຊ້ຜະລິດຕະພັນ
ໂດຍກຳນົດໃຫ້ລູກຄ້ານຳໃຊ້ແພັບເຫຼົ່ານີ້ໂດຍອອກຄ່າໃຊ້ຈ່າຍເອງ.
ພຽງແຕ່ໂດຍການລວມເອົາຫຼັກປະຕິບັດຄວາມປອດໄພໂດຍການອອກແບບເທົ່ານັ້ນທີ່ພວກເຮົາຈະທຳລາຍວົງຈອນອັນໂຫດຮ້າຍຂອງການສ້າງ ແລະ ນຳໃຊ້ການແກ້ໄຂ.

ເພື່ອໃຫ້ບັນລຸມາດຕະຖານການຮັກສາຄວາມປອດໄພຂອງຊອບແວລະດັບສູງນີ້,
ຫນ່ວຍງານຜູ້ສ້າງສະຫນັບສະຫນູນໃຫ້ຜູ້ຜະລິດຈັດລຳດັບຄວາມສຳຄັນຂອງການເຊື່ອມໂຍງຄວາມປອດໄພຂອງຜະລິດຕະພັນເປັນເງື່ອນໄຂເບື້ອງຕົ້ນທີ່ສຳຄັນ ສຳລັບຄຸນສົມບັດ ແລະ ຄວາມໄວໃນການອອກສູ່ຕະຫຼາດ.
ຊ່ອງເວລາຜ່ານໄປ,

[1]ຫນ່ວຍງານຜູ້ຂຽນຍອມວ່າ "ຄວາມປອດໄພ" ມີຫຼາຍຄວາມໝາຍຂຶ້ນກັບສະພາບການທີ່ມັນໃຊ້. ສຳລັບຈຸດປະສົງຂອງຄູ່ມືນີ້, "ຄວາມປອດໄພ" ຈະໝາຍເຖິງການຍົກສະດັບມາດຕະຖານຄວາມປອດໄພດ້ານເຕັກໂນໂລຍີເພື່ອປົກປ້ອງລູກຄ້າຈາກກິດຈະກຳທາງໄຊເບີທີ່ເປັນອັນຕະລາຍ.

ທີມງານວິສະວະກຳຈະສາມາດສ້າງຈັງຫວະການຄົ້ງໂຕແບບໃໝ່ທີ່ຄວາມປອດໄພໄດ້ຮັບການອອກແບບມາຢ່າງແທ້ຈິງ ແລະ ໃຊ້ຄວາມພະຍາຍາມໜ້ອຍລົງໃນການບຳລຸງຮັກສາ.

ຈາກມຸມມອງນີ້,
ສະຫະພາບເອີຣົບໄດ້ເສີມຂະຫຍາຍຄວາມສຳຄັນຂອງຄວາມປອດໄພຂອງຜະລິດຕະພັນໃນກົດໝາຍວ່າດ້ວຍຄວາມຢືດຢຸ່ນທາງໄຊເບີ (Cyber-Resilience-Act),
ໂດຍເນັ້ນໜັກວ່າຜູ້ຜະລິດຄວນໃຊ້ການຮັກສາຄວາມປອດໄພຕະຫຼອດວົງຈອນຊີວິດຂອງຜະລິດຕະພັນ
ເພື່ອປ້ອງກັນບໍ່ໃຫ້ຜູ້ຜະລິດແນະນຳຜະລິດຕະພັນທີ່ມີຄວາມສ່ຽງເຂົ້າສູ່ຕະຫຼາດ.

ເພື່ອສ້າງອະນາຄົດທີ່ເຕັກໂນໂລຢີ ແລະ
ຜະລິດຕະພັນທີ່ປອດໄພທີ່ກ່ຽວຂ້ອງມີຄວາມປອດໄພຫຼາຍຂຶ້ນສຳລັບລູກຄ້າ
ໜ່ວຍງານຜູ້ຂຽນຈຶ່ງຮຽກຮ້ອງໃຫ້ຜູ້ຜະລິດປັບປຸງໂປຣແກຣມການອອກແບບ ແລະ ພັດທະນາໃໝ່
ເພື່ອໃຫ້ຈັດສົ່ງສະເພາະ

ຜະລິດຕະພັນ ຄວາມປອດໄພໂດຍການອອກແບບ ແລະ ຄ່າເລີ້ມຕົ້ນໃຫ້ກັບລູກຄ້າເທົ່ານັ້ນ.
ຜະລິດຕະພັນທີ່ມີຄວາມປອດໄພໂດຍການອອກແບບ
ຄືຜະລິດຕະພັນທີ່ການຮັກສາຄວາມປອດໄພຂອງລູກຄ້າເປັນເປົ້າໝາຍທາງທຸລະກິດຫຼັກ
ບໍ່ແມ່ນພຽງແຕ່ຄຸນລັກສະນະທາງເຕັກນິກເທົ່ານັ້ນ. ຜະລິດຕະພັນທີ່ມີຄວາມປອດໄພໂດຍການອອກແບບ
ເລີ້ມຕົ້ນຈາກເປົ້າໝາກ່ອນທີ່ຈະເລີ່ມການພັດທະນາຜະລິດຕະພັນທີ່ມີຄວາມປອດໄພໂດຍການອອກແບບໂດຍຄ່າເລີ່ມຕົ້ນ ແມ່ນຜະລິດຕະພັນທີ່ປອດໄພໃນການນຳໃຊ້ "ນອກຂອບ"
ໂດຍບໍ່ຈຳເປັນຕ້ອງປ່ຽນແປງການຕັ້ງຄ່າເລັກນ້ອຍ ຫຼື ບໍ່ມີເລີຍ ແລະ
ຄຸນລັກສະນະຄວາມປອດໄພພ້ອມໃຊ້ງານໂດຍບໍ່ມີຄ່າໃຊ້ຈ່າຍເພີ່ມເຕີມ. ເມື່ອເຮັດວຽກຮ່ວມກັນ,
ຫຼັກການສອງຢ່າງນີ້ຊ່ວຍແບ່ງເບົາພາລະໃນການຮັກສາຄວາມປອດໄພໃຫ້ກັບຜູ້ຜະລິດ ແລະ
ຫຼຸດຜ່ອນໂອກາດທີ່ລູກຄ້າຈະຕົກເປັນເຫຍື່ອຂອງເຫດການດ້ານຄວາມປອດໄພທີ່ເປັນຜົນມາຈາກການຕັ້ງຄ່າທີ່ບໍ່ຖືກຕ້ອງ, ການແກ້ໄຂໄວບໍ່ພຽງພໍ ຫຼື ບັນຫາທົ່ວໄປອື່ນໆອີກຫຼວງຫຼາຍ.

ໜ່ວຍງານຄວາມປອດໄພທາງໄຊເບີ ແລະ ໂຄງສ້າງພື້ນຖານ (CISA), ອົງການຄວາມປອດໄພແຫ່ງຊາດ (NSA),
ຫ້ອງການສືບສວນຂອງລັດຖະບານກາງ (FBI) ແລະ ຄູ່ຮ່ວມງານສາກົນຕໍ່ໄປນີ້[2]
ໃຫ້ຄຳແນະນຳໃນຄູ່ມືນີ້ເພື່ອແຈ້ງ
ສຳລັບຜູ້ຜະລິດເຕັກໂນໂລຢີເພື່ອຮັບປະກັນຄວາມປອດໄພຂອງຜະລິດຕະພັນຂອງຕົນ:

- ສູນຄວາມປອດໄພທາງໄຊເບີຂອງອອັສເຕຣເລັຍ (ACSC)

[2] ຕໍ່ໄປນີ້ເອີ້ນວ່າ "ໜ່ວຍງານຜູ້ຂຽນ."

- ສູນຄວາມປອດໄພທາງໄຊເບີຂອງການາດາ (CCCS)
- ສູນຄວາມປອດໄພທາງໄຊເບີແຫ່ງຊາດຂອງສະຫະຣາຊອານາຈັກ (NCSC-UK)
- ສຳນັກງານຄວາມປອດໄພຂໍ້ມູນຂ່າວສານຂອງເຢັຍຣະມັນ (BSI)
- ສູນຄວາມປອດໄພທາງໄຊເບີແຫ່ງຊາດຂອງເນເທີແລນດ໌ (NCSC-NL)
- ທີມງານຕອບໂຕ້ສຸກເສີນດ້ານຄອມພິວເຕີນິວຊີແລນດ໌ (CERT NZ)

ແລະສູນຄວາມປອດໄພທາງໄຊເບີ ແຫ່ງຊາດ ຂອງ ນິວ ຊີແລນດ໌ (NCSC-NZ).

ໜ່ວຍງານຜູ້ຂຽນຮັບຮູ້ການປະກອບສ່ວນຂອງຄູ່ຮ່ວມງານຂອງພາກເອກະຊົນຈຳນວນຫຼາຍໃນການຍົກລະດັບທາງດ້ານຄວາມປອດໄພໂດຍການອອກແບບ ແລະ ຄວາມປອດໄພໂດຍຄ່າເລີ່ມຕົ້ນ.
ເຜະລິດຕະພັນນີ້ແມ່ນມີຈຸດປະສົງເພື່ອກ້າວໄປສູ່ການສົນທະນາລະຫວ່າງປະເທດກ່ຽວກັບບູລິມະສິດທີ່ສຳຄັນ, ການລົງທຶນ ແລະ ການຕັດສິນໃຈທີ່ຈຳເປັນ ເພື່ອໃຫ້ບັນລຸອະນາຄົດທີ່ເຕັກໂນໂລຢີມີຄວາມປອດໄພ, ຄວາມໝັ້ນຄົງ ແລະຄວາມທົນທານໂດຍການອອກແບບ ແລະ ຄ່າເລີ່ມຕົ້ນ. ດ້ວຍເຫດນີ້, ໜ່ວຍງານຜູ້ຂຽນຊອກຫາຄຳຄິດເຫັນກ່ຽວກັບເຜະລິດຕະພັນນີ້ຈາກຜູ້ທີ່ມີສ່ວນໄດ້ສ່ວນເສຍ ແລະ ຕັ້ງໃຈຈະປະຊຸມການຮັບຟັງເປັນຊຸດເພື່ອປັບປຸງ, ລະບຸ ແລະ ພັດທະນາຄຳແນະນຳຂອງພວກເຮົາເພີ້ມເພື່ອບັນລຸເປົ້າໝາຍຮ່ວມກັນ.

ສຳລັບຂໍ້ມູນເພີ່ມເຕີມກ່ຽວກັບຄວາມສຳຄັນຂອງຄວາມປອດໄພຂອງເຜະລິດຕະພັນ, ຈົ່ງເບິ່ງບົດຄວາມຂອງ CISA ຕົ້ນທຶນຂອງເຕັກໂນໂລຢີທີ່ບໍ່ປອດໄພ ແລະ ສິ່ງທີ່ພວກເຮົາສາມາດເຮັດໄດ້ກ່ຽວກັບເຕັກໂນໂລຢີນັ້ນ (The Cost of Unsafe Technology and What We Can Do About It).

ຄວາມປອດໄພໂດຍການອອກແບບ Secure-by-Design

"ຄວາມປອດໄພໂດຍການອອກແບບ"
ໝາຍຄວາມວ່າເຜະລິດຕະພັນເຕັກໂນໂລຢີຖືກສ້າງຂຶ້ນໃນລັກສະນະທີ່ສົມເຫດສົມຜົນ ເພື່ອປ້ອງກັນຜູ້ກະທຳທາງໄຊເບີທີ່ເປັນອັນຕະລາຍໃນການເຂົ້າເຖິງອຸປະກອນ, ຂໍ້ມູນ, ແລະໂຄງສ້າງພື້ນຖານທີ່ເຊື່ອມຕໍ່ໄດ້ສຳເລັດ. ຜູ້ຜະລິດຊອບແວຄວນປະຕິບັດການປະເມີນຄວາມສ່ຽງເພື່ອລະບຸ ແລະ ກຳນົດໄພຂົ່ມຂູ່ທາງໄຊເບີທີ່ກຳລັງພັດທະນາແນວທາງການພັດທະນາເຕັກໂນໂລຊີຂໍ້ມູນຂ່າວສານທີ່ປອດໄພ (IT) ແລະ ການປ້ອງກັນຫຼາຍຊັ້ນ - ເອີ້ນວ່າ ການປ້ອງກັນໃນຊຶ່ງເລິກ - ຍັງແນະນຳເພື່ອປ້ອງກັນກິດຈະກຳຂອງຝ່າຍກົງກັນຂ້າມຈາກການປະນີປະນອມລະບົບ ຫຼື ໄດ້ຮັບການເຂົ້າເຖິງຂໍ້ມູນທີ່ລະອຽດອ່ອນໂດຍບໍ່ໄດ້ຮັບອະນຸຍາດ.
ໜ່ວຍງານຜູ້ຂຽນແນະນຳຜູ້ຜະລິດໃຊ້ແບບຈຳການຂົ່ມຂູ່ທີ່ ປັບແຕ່ງໃນລະຫວ່າງຜະລິດຕະພັນ

ຂັ້ນຕອນການພັດທະນາເພື່ອແກ້ໄຂໄພຂົ່ມຂູ່ທີ່ອາດເກີດຂຶ້ນກັບລະບົບ ແລະ ບັນຊີສຳລັບຂະບວນການ ການນຳໃຊ້ຂອງແຕ່ລະລະບົບ.

ໜ່ວຍງານຜູ້ຂຽນຮຽກຮ້ອງໃຫ້ຜູ້ຜະລິດໃຊ້ວິທີການຮັກສາຄວາມປອດໄພແບບລວມສຳລັບຜະລິດຕະພັນ ແລະ ເວທີຂອງຕົນ ການພັດທະນາທີ່ຄວາມປອດໄພໂດຍການອອກແບບ(Secure-by-Design) ຕ້ອງການລົງທຶນແຫຼ່ງຂໍ້ມູນຈຳນວນຫຼາຍ ໂດຍຜູ້ຜະລິດຊອບແວໃນແຕ່ລະຊັ້ນຂອງຂະບວນການອອກແບບ ແລະ ການພັດທະນາ ຜະລິດຕະພັນທີ່ບໍ່ສາມາດ "ປິດ" ໄດ້ໃນພາຍຫຼັງ.
ຈຳເປັນຕ້ອງມີຄວາມເປັນຜູ້ນຳທີ່ເຂັ້ມແຂງໂດຍຜູ້ບໍລິຫານທຸລະກິດຊັ້ນນຳຂອງຜູ້ຜະລິດ ເພື່ອເຮັດໃຫ້ການຮັກສາຄວາມປອດໄພ ມີຄວາມສຳຄັນທາງທຸລະກິດ, ບໍ່ພຽງແຕ່ເປັນລັກສະນະດ້ານວິຊາການເທົ່ານັ້ນ. ການຮ່ວມມືລະຫວ່າງ ຜູ້ນຳທຸລະກິດ ແລະ ທີມງານດ້ານວິຊາການນີ້ຄວບຄຸມຕັ້ງແຕ່ ຂັ້ນຕອນທຳອິດຂອງການອອກແບບ ແລະ ການພັດທະນາ ໄປຈົນເຖິງການນຳໃຊ້ ແລະ ການບຳລຸງຮັກສາຂອງລູກຄ້າ. ຜູ້ຜະລິດໄດ້ຮັບການສະໜັບສະໜູນໃຫ້ມີແລກປ່ຽນ ແລະ ການລົງທຶນຢ່າງໜັກ, ລວມທັງສິ່ງທີ່ລູກຄ້າຈະ "ເບິ່ງບໍ່ເຫັນ", ເຊັ່ນ:
ການເຄື່ອນຍ້າຍໄປສູ່ພາສາການຂຽນໂປຼແກຼມທີ່ກຳຈັດ. ພວກເຂົາຄວນຈັດລຳດັບຄວາມສຳຄັນຂອງຄຸນສົມບັດ, ກົນໄກ ແລະ ການນຳໃຊ້ເຄື່ອງມືທີ່ປົກປ້ອງລູກຄ້າຫຼາຍກວ່າຄຸນສົມບັດ ຂອງຜະລິດຕະພັນທີ່ເບິ່ງຄືວ່າໜ້າສົນໃຈແຕ່ຂະຫຍາຍຂອບເຂດການໂຈມຕີ.

ບໍ່ມີວິທີແກ້ບັນຫາດຽວທີ່ຈະຢຸດການຄຸກຄາມຂົ່ມຂູ່ຢ່າງຕໍ່ເນື່ອງຂອງຜູ້ປະສົບເຄາະຮ້າຍທາງໄຊເບີທີ່ ທີ່ສວຍໃຊ້ປະໂຫຍດຈາກຊ່ອງໂຫວ່ດ້ານເຕັກໂນໂລຍີ ແລະ ຜະລິດຕະພັນທີ່ "Secure-by-Design" ຈະຍັງຄົງ ປະສົບກັບຊ່ອງໂຫ່ວຕໍ່ໄປ; ແນວໃດກໍ່ຕາມ,
ຊ່ອງໂຫວ່ຈຳນວນຫຼາຍເກີດມາຈາກສາເຫດສ່ວນຍ່ອຍທີ່ຂ້ອນຂ້າງນ້ອຍ.
ຜູ້ຜະລິດຄວນສ້າງແຜນງານເປັນລາຍລັກອັກສອນເພື່ອຈັດ
ກຸ່ມຜະລິດຕະພັນທີ່ມີຢູ່ໃຫ້ສອດຄ່ອງກັບຫຼັກປະຕິບັດຄວາມປອດໄພໂດຍການອອກແບບຫຼາຍຂຶ້ນ ເພື່ອໃຫ້ແນ່ໃຈວ່າຈະປິດເບື້ອນສະເພາະແຕ່ໃນສະຖານະການພິເສດເທົ່ານັ້ນ.

ໜ່ວຍງານຜູ້ຂຽນຮັບຮູ້ວ່າການເປັນເຈົ້າຂອງຜະລິດຕະພັນດ້ານຄວາມປອດໄພສຳລັບລູກຄ້າ ແລະ ການຮັບປະກັນລະດັບຄວາມປອດໄພຂອງລູກຄ້າໃນລະດັບນີ້ອາດຈະເພີ່ມຕົ້ນທຶນໃນການພັດທະນາ.
ຢ່າງໃດກໍ່ຕາມ, ການລົງທຶນໃນແນວການປະຕິບັດ "ຄວາມປອດໄພໂດຍການອອກແບບ"
ໃນຂະນະທີ່ພັດທະນາຜະລິດຕະພັນເຕັກໂນໂລຍີໃໝ່ ແລະ
ການຮັກສາຜະລິດຕະພັນທີ່ມີຢູ່ແລ້ວສາມາດປັບປຸງມາດຕະການຮັກສາຄວາມປອດໄພຂອງລູກຄ້າໄດ້ຢ່າງຫຼວງຫຼາຍແລະ ຫຼຸດຜ່ອນໂອກາດຂອງການຖືກທຳລາຍ.ຫຼັກການຄວາມປອດໄພໂດຍການອອກແບບ

ບໍ່ພຽງແຕ່ຈະເສີມຄວາມເຂັ້ມແຂງໃຫ້ກັບມາດຕະການຮັກສາຄວາມປອດໄພສຳລັບລູກຄ້າ ແລະ ຊື່ສຽງຂອງຍີ່ຫໍ້ສຳລັບຜູ້ຜະລິດໃນໄລຍະຍາວ.
ຂໍ້ແນະນຳສຳລັບຜູ້ຜະລິດຊອບແວທີ່ລະບຸໄວ້ຂ້າງລຸ່ມນີ້ສະແດງບັນຊີລາຍການຂອງແນວທາງປະຕິບັດ ແລະ ນະໂຍບາຍການພັດທະນາຜະລິດຕະພັນທີ່ແນະນຳສຳລັບຜູ້ຜະລິດເພື່ອພິຈາລະນາ.

ຄວາມປອດໄພໂດຍຄ່າເລີ່ມຕົ້ນ Secure-by-Default

ປອດໄພໂດຍຄ່າເລີ້ມຕົ້ນ "ຄວາມປອດໄພໂດຍຄ່າເລີ່ມຕົ້ນ"
ໝາຍເຖິງຜະລິດຕະພັນມີຄວາມທົນທານຕໍ່ກັບຕັກນິກການສະແຫວງຫາຜົນປະໂຫຍດ
ທີ່ແຜ່ຫຼາຍຕັ້ງແຕ່ແກະອອກຈາກກ່ອງໂດຍບໍ່ມີຄ່າໃຊ້ຈ່າຍເພີ່ມເຕີມ. ຜະລິດຕະພັນເຫຼົ່ານີ້ປ້ອງກັນໄພຂົ່ມຂູ່ ແລະ ຄວາມສ່ຽງທີ່ແຜ່ຫຼາຍທີ່ສຸດໂດຍຜູ້ໃຊ້ບາຍທາງບໍ່ຕ້ອງຕ້ອງໃຊ້ຂັ້ນຕອນເພີ່ມເຕີມເພື່ອຮັກສາຄວາມປອດໄພ.
ຜະລິດຕະພັນຄວາມປອດໄພໂດຍຄ່າເລີ້ມຕົ້ນ
ໄດ້ຮັບການແບບມາເພື່ອເຮັດໃຫ້ລູກຄ້າຮັບຮູ້ຢ່າງຈິງຈັງວ່າເມື່ອພວກເຂົາບ່ຽງເບນໄປຈາກຄ່າເລີ່ມຕົ້ນທີ່ປອດໄພ ພວກເຂົາກຳລັງເພີ່ມ ໂອກາດໃນການປະນີປະນອມ
ເວັ້ນເສັຍແຕ່ວ່າພວກເຂົາຈະໃຊ້ການຄວບຄຸມການຊົດເຊີຍເພີ່ມເຕີມ.

- ກຳນົດຄ່າທີ່ປອດໄພຄວນເປັນພື້ນຖານເລີ່ມຕົ້ນ. ຜະລິດຕະພັນຄວາມປອດໄພໂດຍຄ່າເລີ້ມຕົ້ນ ເປີດໃຊ້ງານການຄວບຄຸມຄວາມປອດໄພທີ່ສຳຄັນທີ່ສຸດທີ່ຈຳເປັນໂດຍອັດຕະໂນມັດໃນການປົກປ້ອງອົງກອນ ຈາກຜູ້ກະທຳການທາງໄຊເບີທີ່ເປັນອັນຕະລາຍຕະຫຼອດຈົນໃຫ້ຄວາມສາມາດໃນການນຳໃຊ້ ແລະ ກຳນົດຄ່າການຄວບຄຸມຄວາມປອດໄພເພີ້ມເຕີມໂດຍບໍ່ມີຄ່າໃຊ້ຈ່າຍເພີ່ມເຕີມ.
- ຄວາມຊັບຊ້ອນຂອງການກຳນົດຄວາມປອດໄພບໍ່ຄວນເປັນບັນຫາຂອງລູກຄ້າ. ພະນັກງານໄອທີ (IT) ຂອງອົງກອນມັກມີວຽກງານໜ້າທີ່ຮັບຜິດຊອບດ້ານຄວາມປອດໄພ ແລະ ການປະຕິບັດການຫຼາຍເກີນໄປ, ດັ່ງນັ້ນຈຶ່ງເຮັດໃຫ້ມີເວລາຈຳກັດໃນການທຳຄວາມເຂົ້າໃຈ ແລະ ບັບໃຊ້ຜົນກະທົບດ້ານຄວາມປອດໄພ ແລະ ການຫຼຸດຜ່ອນທີ່ຈຳເປັນສຳລັບມາດຕະການຮັກສາຄວາມປອດໄພທາງໄຊເບີທີ່ມີປະສິດທິພາບ.
  ໂດຍຜ່ານການເພີ່ມປະສິດທິພາບການກຳນົດຄ່າຜະລິດຕະພັນທີ່ປອດໄພ -
  ຮັກສາຄວາມປອດໄພ"ເສັ້ນທາງເລີ່ມຕົ້ນ" -
  ຜູ້ຜະລິດສາມາດຊ່ວຍລູກຄ້າຂອງຂອງຕົນໄດ້ໂດຍການເຮັດຄວາມເຂົ້າໃຈວ່າ
  ຜະລິດຕະພັນຂອງຕົນໄດ້ຮັບການຜະລິດ, ແຈກຢາຍ, ແລະ ນຳໃຊ້ຢ່າງປອດໄພຕາມມາດຕະຖານ
  "ຄວາມປອດໄພໂດຍຄ່າເລີ້ມຕົ້ນ".

ຜູ້ຜະລິດຜະລິດຕະພັນທີ່ເປັນ "ຄວາມປອດໄພໂດຍຄ່າເລີ້ມຕົ້ນ"
ບໍ່ຄິດຄ່າບໍລິການເພີ່ມເຕີມສຳລັບການຕິດຕັ້ງການກຳນົດຄ່າຄວາມປອດໄພເພີ່ມເຕີມ
ແຕ່ຈະລວມເອົາໄວ້ຢູ່ໃນຜະລິດຕະພັນພື້ນຖານເຊັ່ນ: ສາຍແອວນິລະໄພທີ່ມີຢູ່ໃນລົດຍົນໃໝ່ທຸກຄັນ.

ການຮັກສາຄວາມປອດໄພບໍ່ແມ່ນທາງເລືອກທີ່ທັນສະໄໝແຕ່ໃກ້ຄຽງກັບມາດຕະຖານທີ່ລູກຄ້າທຸກຄົນຄວນຄາດຫວັງໂດຍບໍ່ມີການເຈລະຈາ ຫຼື ຈ່າຍເງິນເພີ່ມ.

ຄຳແນະນຳສຳລັບຜູ້ຜະລິດຊອັບແວ

ຄູ່ມືຮ່ວມນີ້ໃຫ້ຄຳແນະນຳກັບຜູ້ຜະລິດສຳລັບການພັດທະນາແຜນງານທີ່ເປັນລາຍລັກອັກສອນເພື່ອນຳໄປປະຕິບັດແລະ ຮັບປະກັນຄວາມປອດໄພດ້ານໄອທີ (IT).
ໜ່ວຍງານຜູ້ຂຽນແນະນຳໃຫ້ຜູ້ຜະລິດຊອັບແວໃຊ້ກົນລະຍຸດທີ່ລະບຸໄວ້ໃນພາກສ່ວນຂ້າງລຸ່ມນີ້ເພື່ອເປັນເຈົ້າຂອງຜະລິດຕະພັນດ້ານຄວາມປອດໄພຂອງລູກຄ້າຜ່ານຫຼັກການ Secure-by-Design and -Default (ປອດໄພໂດຍການອອກແບບ ແລະ - ຄ່າເລີ້ມຕົ້ນ).

ຫຼັກການຮັກສາຄວາມປອດໄພຂອງຜະລິດຕະພັນຊອັບແວ

ຜູ້ຜະລິດເຕັກໂນໂລຢີໄດ້ຮັບການສະໜັບສະໜູນໃຫ້ຮັບຮອງເອົາຈຸດສຸມຍຸດທະສາດທີ່ໃຫ້ຄວາມສຳຄັນກັບຄວາມປອດໄພຂອງຊອັບແວ.
ໜ່ວຍງານຜູ້ຂຽນໄດ້ພັດທະນາສາມຫຼັກການສຳຄັນຂ້າງລຸ່ມນີ້ເພື່ອເປັນແນວທາງໃຫ້ແກ່ຜູ້ຜະລິດຊອັບແວໃນການສ້າງຄວາມປອດໄພຂອງຊອັບແວເຂົ້າໃນຂະບວນການອອກແບບກ່ອນທີ່ຈະພັດທະນາ, ຕັ້ງຄ່າ ແລະ ການຈັດສົ່ງຜະລິດຕະພັນຂອງຕົນ.

1. ພາລະດ້ານຄວາມປອດໄພບໍ່ຄວນຕົກຢູ່ນຳ ລູກຄ້າແຕ່ພຽງຜູ້ດຽວ. ຜູ້ຜະລິດຊອັບແວຄວນເປັນເຈົ້າຂອງຜະລິດຕະພັນດ້ານຄວາມປອດໄພຂອງການຊື້ຂອງລູກຄ້າ ແລະ ພັດທະນາຜະລິດຕະພັນຂອງຕົນຕາມນັ້ນ.
2. ຍອມຮັບຄວາມໂປ່ງໃສ ແລະ ຄວາມຮັບຜິດຊອບທີ່ຮຸນແຮງ.
   ຜູ້ຜະລິດຊອັບແວຄວນມີຄວາມພາກພູມໃຈໃນການນຳສະເໜີຜະລິດຕະພັນທີ່ປອດໄພ ແລະ ໝັ້ນຄົງ, ລວມເຖິງສ້າງຄວາມແຕກຕ່າງໃຫ້ກັບຊຸມຊົນຜູ້ຜະລິດອື່ນໆ ຕາມຄວາມສາມາດຂອງຕົນ.
   ນີ້ອາດຈະລວມເຖິງການແບ່ງປັນຂໍ້ມູນທີ່ພວກເຂົາຮຽນຮູ້ຈາກການເຮັດໃຫ້ໃຊ້ການໄດ້ຂອງລູກຄ້າເຊັ່ນການຍອມຮັບກົນໄກການພິສູດຕົວຕົນທີ່ຮັດກຸມຕາມຄ່າເລີ່ມຕົ້ນ.
   ນອກຈາກນີ້ຍັງລວມເຖິງຄວາມມຸ່ງໝັ້ນທີ່ແຮງກ້າທີ່ຈະຮັບປະກັນວ່າການຄ້ຳແນະນຳກ່ຽວກັບຊ່ອງໂຫວ່ ແລະ ບັນທຶກຄວາມສ່ຽງທົ່ວໄປ ແລະ ຄວາມສ່ຽງທີ່ກ່ຽວຂ້ອງ(CVE) ນັ້ນແມ່ນຄົບຖ້ວນສົມບູນ ແລະ ຖືກຕ້ອງ. ຢ່າງໃດກໍຕາມ, ຈົ່ງລະວັງຂອງການລໍ້ລວງໃຫ້ນັບ CVEs ເປັນເມຕຣິກທາງລົບ, ເນື່ອງຈາກວ່າຕົວເລກດັ່ງກ່າວຍັງເປັນສັນຍານຂອງການວິເຄາະລະຫັດທີ່ດີ ແລະ ການທົດສອບຊຸມຊົນ.
3. ສ້າງໂຄງປະກອບການອົງກອນ ແລະ ຄວາມເປັນຜູ້ນຳເພື່ອບັນລຸເປົ້າໝາຍດັ່ງກ່າວ.
   ໃນຂະນະທີ່ຄວາມຊ່ຽວຊານທາງດ້ານເຕັກນິກມີຄວາມສຳຄັນຕໍ່ຄວາມປອດໄພຂອງຜະລິດຕະພັນ,

ແຕ່ຜູ້ບໍລິຫານລະດັບສູງກໍ່ເປັນຜູ້ມີອຳນາດຕັດສິນໃຈຫຼັກໃນການກຳເນີນການປ່ຽນແປງໃນອົງກອນ.
ຄວາມມຸ່ງໝັ້ນລະດັບຜູ້ບໍລິຫານສຳລັບຜູ້ຜະລິດຊອັບແວໃນການຈັດລຳດັບຄວາມສຳຄັນຂອງການຮັກສ
າຄວາມປອດໄພເປັນອົງປະກອບທີ່ສຳຄັນຂອງການພັດທະນາຜະລິດຕະພັນ
ຈຳເປັນຕ້ອງໃຫ້ມີການພັດທະນາການຮ່ວມມືກັບລູກຄ້າຂອງອົງກອນເພື່ອທຳຄວາມເຂົ້າໃຈ:

ກ. ການແນະນຳສະຖານະການນຳໃຊ້ຜະລິດຕະພັນພ້ອມກັບຮູບແບບໄພຂົ່ມຂູ່ທີ່ປັບແຕ່ງມາ

ຂ. ການດຳເນີນການທີ່ສະເໜີສຳລັບການຄວບຄຸມຄວາມປອດໄພເພື່ອໃຫ້ສອດຄ່ອງກັບຫຼັກການ
ຄວາມປອດໄພໂດຍຄ່າເລີ່ມຕົ້ນ

ຄ. ຍຸດທະສາດການຈັດສັນແຫຼ່ງຂໍ້ມູນທີ່ເໝາະສົມກັບຂະໜາດຂອງບໍລິສັດ ແລະ
ຄວາມສາມາດໃນ
ການປ່ຽນແທນແນວທາງປະຕິບັດດ້ານການພັດທະນາແບບເກົ່າດ້ວຍແນວທາງປະຕິບັດທີ່
ຄວາມປອດໄພໂດຍການອອກແບບ

ງ. ຄວາມຕ້ອງການທີ່ຈະຮັກສາສາຍການສື່ສານແບບເປີດສຳລັບຄຳຄິດຄຳເຫັນພາຍໃນ ແລະ
ພາຍນອກ (ເຊັ່ນຄວາມຄິດເຫັນຂອງພະນັກງານ ແລະ ລູກຄ້າ)
ກ່ຽວກັບບັນຫາດ້ານຄວາມປອດໄພຂອງຜະລິດຕະພັນ.
ຄວນເນັ້ນຄວາມປອດໄພຂອງຊອັບແວໃນເວທີສົນທະນາພາຍໃນ (ເຊັ່ນ ກະເປົ໋າມືຫົ່ງຫຼື
ຖົ່ງສີນ້ຳຕານ), ເຊັ່ນດຽວກັນກັບການຕະຫຼາດຜະລິດຕະພັນພາຍນອກ ແລະ
ການມີສ່ວນຮ່ວມຂອງລູກຄ້າ.

ຈ. ການອັດແທກປະສິດຕິພາບພາຍໃນການນຳໃຊ້ຂອງລູກຄ້າ.
ຜູ້ບໍລິຫານລະດັບສູງຈະຕ້ອງການທີ່ຈະຮູ້ວ່າການລົງທຶນດ້ານການຮັກສາຄວາມປອດໄພໂດຍກາ
ນອອກແບບ ແລະ ຄ່າເລີ່ມຕົ້ນ
ຈະຊ່ວຍເຫຼືອລູກຄ້າໄດ້ໃນດ້ານໃດແດ່ໂດຍເຮັດໃຫ້ແພດຄວາມປອດໄພຊ້ຳລົງ,
ຫຼຸດຜ່ອນຄວາມຜິດພາດໃນການຕັ້ງຄ່າ ແລະ
ຫຼຸດຜ່ອນໜ້າການໂຈມຕີໃຫ້ເຫຼືອໜ້ອຍທີ່ສຸດ.ເພື່ອເຮັດໃຫ້ສາມຫຼັກການນີ້ໃຊ້ການໄດ້,
ຜູ້ຜະລິດຄວນພິຈາລະນາວິທີໃນການປະຕິບັດງານຫຼາຍປະການເພື່ອພັດທະນາຂະບວນການພັ
ດທະນາຂອງຕົນ.

ຈັດກອງປະຊຸມຕາມປົກກະຕິກັບຜູ້ບໍລິຫານລະດັບສູງຂອງບໍລິສັດເພື່ອຊຸກຍູ້ຄວາມສຳຄັນຂອງ
ຄວາມປອດໄພໂດຍການອອກແບບແລະ ຄວາມປອດໄພຕາມຄ່າເລີ່ມຕົ້ນພາຍໃນອົງກອນ.
ຄວນກຳນົດນະໂຍບາຍ ແລະ
ລະບຽບປະຕິບັດເພື່ອມອບລາງວັນໃຫ້ທີມງານຜະລິດທີ່ພັດທະນາຜະລິດຕະພັນທີ່ປະຕິບັດຕາມຫຼັກການເຫຼົ່ານີ້

ເຊິ່ງອາດປະກອບມີລາງວັນສໍາລັບການໃຊ້ແນວທາງປະຕິບັດດ້ານຄວາມປອດໄພຊັ້ນແອທີ່ໂດດເດັ່ນ ຫຼື ແຮງຈູງໃຈສໍາລັບຂັ້ນໄດວຽກງານ ແລະ ເງື່ອນໄຂການເລື່ອນຕໍາແໜ່ງ.
ໃຫ້ຄວາມສໍາຄັນກ່ຽວກັບ ຄວາມປອດໄພຂອງຊັ້ນແວເພື່ອຄວາມສໍາເລັດຂອງທຸລະກິດ. ຕົວຢ່າງເຊັ່ນ ພິຈາລະນາແຕ່ງຕັ້ງ "ຜູ້ນໍາດ້ານຄວາມປອດໄພຂອງຊັ້ນແວ" ຫຼື "ທີມຮັກສາຄວາມປອດໄພຂອງຊັ້ນແວ" ທີ່ສະໜັບສະໜູນແນວທາງປະຕິບັດທຸລະກິດ ແລະ ໄອທີ (IT).
ເພື່ອເຊື່ອມຕໍ່ມາດຕະຖານຄວາມປອດໄພຂອງຊັ້ນແວ ແລະ ຄວາມຮັບຜິດຊອບຂອງຜູ້ຜະລິດໂດຍກົງ.
ຜູ້ຜະລິດຄວນກວດສອບໃຫ້ແນ່ໃຈວ່າພວກເຂົາມີໂຄງການການປະເມີນ ແລະ ປະເມີນຄວາມປອດໄພຂອງຜະລິດຕະພັນທີ່, ເປັນເອກະລາດ ແລະ ເຂັ້ມແຂງ ສໍາລັບຜະລິດຕະພັນຂອງຕົນ.
ໃຊ້ຮູບແບບໄພຂົ່ມຂູ່ທີ່ປັບແຕ່ງມາໃນລະຫວ່າງການພັດທະນາເພື່ອຈັດລໍາດັບຄວາມສໍາຄັນສູງສຸດ ແລະ ຜົນກະທົບສູງທີ່ສຸດ

ສິນຄ້າ. ແບບຈໍາລອງໄພຂົ່ມຂູ່ຈະພິຈາລະນາກໍລະນີການນໍາໃຊ້ຈຸດສະເພາະຂອງຜະລິດຕະພັນ ແລະ ຊ່ວຍໃຫ້ທີມງານພັດທະນາສ້າງຄວາມເຂັ້ມແຂງໃຫ້ກັບຜະລິດຕະພັນໄດ້. ປະກາດສຸດທ້າຍ, ຜູ້ນໍາລະດັບສູງຄວນໃຫ້ທີມງານຮັບຜິດຊອບໃນການສົ່ງມອບຜະລິດຕະພັນທີ່ປອດໄພຊຶ່ງເປັນອົງປະກອບທີ່ສໍາຄັນທີ່ດີເລີດ ແລະ ຄຸນນະພາບຂອງຜະລິດຕະພັນ.

ຍຸດທະວິທີທີ່ປອດໄພໂດຍການອອກແບບ Secure-by-Design Tactics

ກອບການພັດທະນາຊັ້ນແວທີ່ປອດໄພ (SSDF), ເຊິ່ງເອີ້ນກັນວ່າ ສະຖາບັນມາດຕະຖານ ແລະ ເຕັກໂນໂລຊີແຫ່ງຊາດ (NIST) SP 800-218
ແມ່ນຊຸດຫຼັກຂອງແນວທາງປະຕິບັດໃນການພັດທະນາຊັ້ນແວທີ່ປອດໄພລະດັບສູງທີ່ສາມາດລວມເຂົ້າໃນແຕ່ລະຂັ້ນຕອນຂອງວົງຈອນຊີວິດການພັດທະນາຊັ້ນແວ (SDLC).
ການປະຕິບັດຕາມແນວທາງປະຕິບັດເຫຼົ່ານີ້ສາມາດຊ່ວຍໃຫ້ຜູ້ຜະລິດຊັ້ນແວມີປະສິດຕິພາບຫຼາຍຂຶ້ນໃນການຄົ້ນຫາ ແລະ ກໍາຈັດຊ່ອງໂຫວ່ໃນຊັ້ນແວທີ່ເຜີຍແຜ່,
ຫຼຸດຜ່ອນຜົນກະທົບທີ່ອາດເກີດຂຶ້ນຈາກການໃຊ້ປະໂຫຍດຈາກຊ່ອງໂຫວ່ ແລະ ແກ້ໄຂສາເຫດຂອງຊ່ອງໂຫວ່ເພື່ອປ້ອງກັນການເກີດຊ້ໍາອີກໃນອະນາຄົດ.
ໜ່ວຍງານຜູ້ຂຽນສະໜັບສະໜູນໃຫ້ໃຊ້ຍຸດທະວິທີທີ່ຄວາມປອດໄພໂດຍການອອກແບບ ລວມທັງຫຼັກການທີ່ອ້າງອີງເຖິງແນວທາງປະຕິບັດ SSDF.
ຜູ້ຜະລິດຊັ້ນແວຄວນພັດທະນາແຜນງານທີ່ເປັນລາຍລັກອັກສອນເພື່ອຮັບຮອງເອົາການປະຕິບັດການພັດທະນາຊັ້ນແວ ຄວາມປອດໄພໂດຍການອອກແບບໄປໃຊ້ມນໜ້າທີ່ການງານຂອງຕົນ
ຕໍ່ໄປນີ້ແມ່ນລາຍການແນວທາງປະຕິບັດທີ່ດີທີ່ສຸດຂອງແຜນກົນລະຍຸດທີ່ມີຮູບພາບປະກອບໂດຍສັງເກດ:

- ພາສາການຂຽນໂປຣແກຣມທີ່ປອດໄພຂອງໜ່ວຍຄວາມຈຳ (SSDF PW.6.1):
  ກຳນົດລຳດັບຄວາມສຳຄັນໃນການນຳໃຊ້ພາສາທີ່ປອດໄພຂອງໜ່ວຍຄວາມຈຳໃນບ່ອນທີ່ເປັນໄປໄດ້.
  ໜ່ວຍງານຜູ້ຂຽນຮັບຮູ້ວ່າການຫຼຸດຜ່ອນຄວາມຈຳສະເພາະອື່ນໆ, ເຊັ່ນການຈັດວາງທີ່ຢູ່ທີ່ຢູ່ແບບສຸ່ມ (ASLR), ຄວາມສົມບູນຂອງການຄວບຄຸມ (CFI), ແລະ ການທົດສອບຊອບແວອັດຕະໂນມັດ(fuzzing) ແມ່ນເປັນປະໂຫຍດສຳລັບຖານລະຫັດດັ້ງເດີມ,
  ແຕ່ບໍ່ພຽງພໍທີ່ຈະຖືກເບິ່ງວ່າເປັນປອດໄພຈາກການອອກແບບຄືກັບທີ່ພວກເຂົາເຮັດ.
  ບໍ່ປ້ອງກັນການສະແຫວງຫາຜົນປະໂຫຍດຢ່າງພຽງພໍ. ຕົວຢ່າງຂອງພາສາທີ່ປອດໄພສຳລັບ
  ໜ່ວຍຄວາມຈຳທີ່ທັນສະໄໝລວມມີ C#, Rust, Ruby, Java, Go, ແລະ Swift. ອ່ານເອກະສານຂໍ້ມູນ
  ໜ່ວຍຄວາມຈຳຂອງ NSA ສຳລັບຂໍ້ມູນເພີ່ມເຕີມ
- ພື້ນຖານຮາດແວທີ່ປອດໄພ:
  ລວມເອົາຄຸນສົມບັດທາງສະຖາປັດຕະຍະກຳທີ່ເປີດໃຊ້ງານການປ້ອງກັນໜ່ວຍຄວາມຈຳແບບລະອຽດ,
  ເຊັ່ນທີ່ ອະທິບາຍໄວ້ໃນ ຄຳແນະນຳ RISC ທີ່ປັບປຸງຄວາມສາມາດຂອງຮາດແວ (CHERI)
  ທີ່ສາມາດຂະຫຍາຍສະຖາປັດຕະຍະກຳຄຳຊຸດຄຳສັ່ງຮາດແວ (ISAs) ແບບເກົ່າໄດ້.
  ສຳລັບຂໍ້ມູນເພີ່ມເຕີມຈົ່ງເຂົ້າເບິ່ງໜ້າເວັບ, CHERI ຂອງມະຫາວິທະຍາໄລແຄມບຣິດຈ໌
- ອົງປະກອບຊອບແວທີ່ປອດໄພ (SSDF PW 4.1): ໄດ້ຮັບ ແລະ
  ບຳລຸງຮັກສາອົງປະກອບຊອບແວທີ່ມີການ

ຮັກສາ ອັດຕະໂນມັດເພື່ອຫຼີກລ່ຽງການໂຈມຕີເວັບເຊັ່ນ: ການຂຽນສະຄຣິບຂ້າມໄຊ.

- ຂໍ້ຄວາມຄົ້ນຫາແບບກຳນົດ ພາຣາມິເຕີຣ໌ (SSDF PW 5.1):
  ໃຊ້ຂໍ້ຄວາມຄົ້ນຫາແບບພາຣາມິເຕີຣ໌ແທນການລວມເອົາການປ້ອນຂໍ້ມູນຂອງຜູ້ໃຊ້ເຂົ້າໃນຂໍ້ຄວາມຄົ້ນ
  ຫາ ເພື່ອຫຼີກເວັ້ນການໂຈມຕີ SQLການທົດສອບຄວາມປອດໄພຂອງແອັບພລິເຄຊັນແບບຄົງທີ່ ແລະ
  ແບບເຄື່ອນໄຫວ (SAST/DAST) (SSDF PW.7.2, PW.8.2):
- ໃຊ້ເຄື່ອງມືເຫຼົ່ານີ້ເພື່ອວິເຄາະລະຫັດແຫຼ່ງຂອງຜະລິດຕະພັນ ແລະ
  ພຶດຕິກຳຂອງແອັບພລິເຄຊັນເພື່ອກວດຫາແນວທາງປະຕິບັດທີ່ມັກມີຄວາມຜິດພາດ.
  ເຄື່ອງມືເຫຼົ່ານີ້ຄວບຄຸມບັນຫາຕ່າງໆ
  ຕັ້ງແຕ່ການຈັດການໜ່ວຍຄວາມຈຳທີ່ບໍ່ເໝາະສົມຈົນເຖິງການສ້າງແບບສືບຄົ້ນຖານຂໍ້ມູນທີ່ມີຂໍ້ຜິດພາ
  ດ (ເຊັ່ນ: ການປ້ອນຂໍ້ມູນຂອງຜູ້ໃຊ້ທີ່ບໍ່ໄດ້ຮັບການແກ້ໄຂທີ່ນຳໄປສູ່ການແຊກແຊງຂອງ SQL). ເຄື່ອງມື
  SAST ແລະ DAST ສາມາດລວມເຂົ້າໃນຂະບວນການພັດທະນາ ແລະ
  ດຳເນີນການໂດຍອັດຕະໂນມັດໂດຍເປັນສ່ວນໜຶ່ງຂອງການພັດທະນາຊອບແວ. SAST ແລະ DAST
  ຄວນເສີມການທົດສອບປະເພດອື່ນໆ ເຊັ່ນການທົດສອບ ໜ່ວຍງານ ແລະ

ການທົດສອບການລວມເພື່ອໃຫ້ແນ່ໃຈວ່າຜະລິດຕະພັນເປັນໄປຕາມຂໍ້ກຳນົດດ້ານຄວາມປອດໄພທີ່ຄາດໄວ້. ເມື່ອບັນຫາຖືກລະບຸ ຜູ້ຜະລິດຄວນທຳການວິເຄາະສາເຫດທີ່ແທ້ຈິງເພື່ອແກ້ໄຂຈຸດອ່ອນທີ່ເປັນລະບົບ.

- ການກວດສອບລະຫັດ (SSDF PW.7.1, PW.7.2):
  ພະຍາຍາມເຮັດໃຫ້ແນ່ໃຈວ່າລະຫັດທີ່ສົ່ງເຂົ້າໄປໃນຜະລິດຕະພັນຜ່ານການທົບທວນຄືນຈາກຜູ້ພັດທະນາອື່ນໆ ເພື່ອໃຫ້ໝັ້ນໃຈໃນຄຸນນະພາບທີ່ສູງຂຶ້ນ.
- ລາຍການວັດສະດຸຂອງຊອບແວ Software Bill of Materials (SBOM) (SSDF PS.3.2, PW.4.1): ລວມການສ້າງ SBOM[3] ເພື່ອໃຫ້ເບິ່ງເຫັນເຂົ້າໄປໃນຊຸດຂອງຊອບແວທີ່ເຂົ້າສູ່ຜະລິດຕະພັນ.
- ໂປຣແກຣມເປີດເຜີຍຊ່ອງໂຫວ່ (SSDF RV.1.3):
  ຈັດສ້າງໂປຣແກຣມເປີດເຜີຍຊ່ອງໂຫວ່ທີ່ຊ່ວຍໃຫ້ນັກຄົ້ນຄວ້າດ້ານຄວາມປອດໄພສາມາດລາຍງານເລື້ອງຊ່ອງໂຫວ່ ແລະ ໄດ້ຮັບຄວາມຄຸ້ມຄອງທາງດ້ານກົດໝາຍໃນການດຳເນີນການດັ່ງກ່າວ.
  ໃນສ່ວນຫນຶ່ງຂອງສິ່ງນີ້, ຜູ້ສະໜອງຄວນສ້າງຂະບວນການເພື່ອກຳນົດສາເຫດຂອງຊ່ອງໂຫວ່ທີ່ຄົ້ນພົບ. ຂະບວນການດັ່ງກ່າວຄວນຮວມເຖິງການກຳນົດວ່າ
  ການໃຊ້ແນວທາງປະຕິບັດຄວາມປອດໄພໂດຍການອອກແບບໃນເອກະສານນີ້ (ຫຼື ແນວທາງປະຕິບັດທີ່ຄ້າຍຄືກັນອື່ນໆ) ຈະເປັນການສະກັດກັ້ນການແນະນຳຊ່ອງໂຫວ່ ຫຼື ບໍ່.
- ຄວາມສົມບູນຂອງ CVE: ກວດສອບໃຫ້ແນ່ໃຈວ່າ CVEs ທີ່ຖືກເຜີຍແຜ່ມີສາເຫດອັນແທ້ຈິງ ຫຼື ການຄົດໄລ່ຈຸດອ່ອນທົ່ວໄປ (CWE) ເພື່ອເຮັດໃຫ້ສາມາດວິເຄາະ
  ສາເຫດຄວາມປອດໄພຂອງຊອບແວທົ່ວທັງອຸດສາຫະກຳໄດ້. ໃນຂະນະທີ່ການຮັບປະກັນວ່າ CVE ທຸກໆລາຍການແມ່ນຖືກຕ້ອງແລະ ຄົບຖ້ວນອາດໃຊ້ເວລາເພີ້ມຂຶ້ນ
  ແຕ່ມັນກໍຈະຊ່ວຍໃຫ້ໜ່ວຍງານທີ່ແຕກຕ່າງກັນສາມາດສັງເກດເຫັນແນວໂນ້ມຂອງອຸດສາຫະກຳທີ່ມີປະໂຫຍດຕໍ່ຜູ້ຜະລິດ ແລະ ລູກຄ້າທຸກຄົນ. ສຳລັບຂໍ້ມູນເພີ່ມເຕີມກ່ຽວກັບການຈັດການຊ່ອງໂຫວ່, ຈົ່ງເບິ່ງຄຳແນະນຳ SVCC ສະເພາະ ຜູ້ມີສ່ວນໄດ້ສ່ວນເສຍຂອງ CISA (CISA's Stakeholder-specific SVCC guidance).
- ອອກແບບໂຄງສ້າງພື້ນຖານເພື່ອໃຫ້ການປະນີປະນອມຂອງການຄວບຄຸມຄວາມປອດໄພອັນດຽວບໍ່ໄດ້ສົ່ງຜົນໃຫ້ລະບົບທັງໝົດຖືກປະນີປະນອມ. ຕົວຢ່າງວ່າ
  ການຮັບປະກັນວ່າສິດທິຂອງຜູ້ໃຊ້ແມ່ນຖືກຈັດຫາຢ່າງຈຳກັດ ແລະ ມີການໃຊ້ລາຍການຄວບຄຸມການເຂົ້າເຖິງສາມາດຫຼຸດຜ່ອນຜົນກະທົບຂອງບັນຊີທີ່ຖືກບຸກບຸກໄດ້. ນອກຈາກນີ້, ເຕັກນິກ ແຊນບອັກຊິງ (sandboxing)
  ຊອບແວສາມາດກັກກັນຊ່ອງໂຫວ່ເພື່ອຈຳກັດການປະນີປະນອມຂອງແອັບພລິເຄຊັນທັງໝົດ.

[3] ໜ່ວຍງານຜູ້ຂຽນບາງແຫ່ງກຳລັງຊອກຫາວິທີທາງອື່ນເພື່ອໃຫ້ໄດ້ຮັບການຮັບປະກັນຄວາມປອດໄພໃນທົ່ວຕ່ອງໂສ້ ການສະໜອງຊອບແວ.

- ບັນລຸເປົ້າໝາຍປະສິດທິພາບທາງໄຊເບີ (CPGs):
  ອອກການປ້ອງກັນໃນເຊີ່ງເລີກແບບຜະລິດຕະພັນທີ່ຕ່ຳຕຸ້ກປະຕິບັດດ້ານຄວາມປອດໄພຂັ້ນພື້ນຖານ.
  ເປົ້າໝາຍປະສິດທິພາບຄວາມປອດໄພທາງໄຊເບີ(Cybersecurity Performance Goals) ຂອງ CISA
  ຊີ້ແຈງພື້ນຖານ ມາດຕະການຄວາມປອດໄພທາງໄຊເບີພື້ນຖານທີ່ອົງກອນຄວນນຳໄປປະຕິບັດ.
  ນອກຈາກນັ້ນ, ສຳລັບວິທີການເພີ່ມເຕີມເພື່ອເສີມສ້າງທ່າທາງຂອງອົງກອນ,
  ຈົ່ງເບິ່ງກອບການປະເມີນທາງໄຊເບີຂອງເປົ້າໝາຍການປະຕິບັດຄວາມປອດໄພທາງໄຊເບີຂອງປະເທດອັງ
  ກິດ
  ເຊິ່ງແບ່ງປັນຄວາມຄ້າຍຄືກັນກັບ CPGs ຂອງ CISA. ຖ້າຜູ້ຜະລິດບໍ່ປະຕິບັດຕາມ CPGs -
  ເຊັ່ນວ່າບໍ່ຮຽກຮ້ອງໃຫ້ມີການກວດສອບຄວາມຖືກຕ້ອງດ້ວຍຫຼາຍປັດໃຈທີ່ປ້ອງກັນຕໍ່ຜິດຊິງສຳລັບພະນັ
  ກງານທຸກຄົນກໍຈະບໍ່ຖືກເຫັນວ່າເປັນການສົ່ງມອບຜະລິດຕະພັນຄວາມປອດໄພໂດຍການອອກແບບ.
  ໜ່ວຍງານຜູ້ຂຽນຮັບຮູ້ວ່າການປ່ຽນແປງເຫຼົ່ານີ້ແມ່ນການປ່ຽນແປງທີ່ສຳຄັນໃນທ່າທາງຂອງອົງກອນ.
  ດັ່ງນັ້ນ, ການແນະນຳຂອງພວກເຂົາຄວນຈະຖືກຈັດລຳດັບຄວາມສຳຄັນຕາມຄວາມສຳຄັນ,
  ຄວາມຊັບຊ້ອນ ແລະ ຜົນກະທົບທາງທຸລະກິດ.
  ແນວທາງປະຕິບັດເຫຼົ່ານີ້ສາມາດຖືກນຳໄປໃຊ້ກັບຊອັບແວໃໝ່ ແລະ ຂະຫຍາຍເພີ່ມຂຶ້ນເພື່ອໃຫ້ຄອບຄຸມ
  ກໍລະນີການນຳໃຊ້ ແລະ ຜະລິດຕະພັນເພີ່ມເຕີມ. ໃນບາງກໍລະນີ ທ່າທາງວິກິດ ແລະ
  ຄວາມສ່ຽງຂອງຜະລິດຕະພັນໃດໜຶ່ງອາດຈະສົມຄວນກັບຕາຕະລາງເວລາທີ່ຂ້ຽງເພື່ອຮັບຮອງເອົາແນວປ
  ະຕິບັດເຫຼົ່ານີ້ໄປໃຊ້. ໃນບັນດາສິ່ງອື່ນໆ, ແນວປະຕິບັດສາມາດຖືກນຳໄປປັບໃຊ້ໃນຖານລະຫັດເດີມ ແລະ
  ປັບປຸງແກ້ໄຂເມື່ອເວລາຜ່ານໄປ.

ຍຸດທະວິທີທີ່ປອດໄພໂດຍຄ່າເລີ່ມຕົ້ນ Secure-by-Default Tactics

ນອກເໜືອຈາກການຮັບຮອງເອົາແນວທາງການພັດທະນາປອດໄພໂດຍການອອກແບບມາໃຊ້ແລ້ວ,
ໜ່ວຍງານຜູ້ຂຽນຍັງແນະນຳໃຫ້ຜູ້ຜະລິດຊອັບແວຈັດລຳດັບ ຄວາມສຳຄັນຂອງການກຳນົດຄ່າ
ຄວາມປອດໄພຕາມຄ່າເລີ່ມຕົ້ນໃນຜະລິດຕະພັນຂອງຕົນ.
ສິ່ງເຫຼົ່ານີ້ຄວນພະຍາຍາມປັບປຸງຜະລິດຕະພັນເພື່ອໃຫ້ສອດຄ່ອງກັບແນວທາງປະຕິບັດເຫຼົ່ານີ້ເມື່ອໄດ້ຮັບການປັບ
ປຸງໃໝ່. ຍົກຕົວຢ່າງ:

- ລົບລ້າງລະຫັດຜ່ານເລີ່ມຕົ້ນ:
  ຜະລິດຕະພັນບໍ່ຄວນມາພ້ອມກັບລະຫັດຜ່ານເລີ່ມຕົ້ນທີ່ທີ່ໃຊ້ຮ່ວມກັນໃນລະດັບສາກົນ.
  ເພື່ອລົບລ້າງລະຫັດຜ່ານເລີ່ມຕົ້ນ,
  ໜ່ວຍງານຜູ້ຂຽນແນະນຳຜະລິດຕະພັນທີ່ຕ້ອງການໃຫ້ຜູ້ບໍລິຫານຕັ້ງລະຫັດຜ່ານທີ່
  ຮັດກຸມໃນລະຫວ່າງການຕິດຕັ້ງ ແລະ ການຕັ້ງຄ່າ.

- ອະຄະຕິການຮັບຮອງຄວາມຖືກຕ້ອງດ້ວຍຫຼາຍປັດໃຈ(MFA)
  ສຳລັບຜູ້ໃຊ້ທີ່ໄດ້ຮັບສິດທິພິເສດ. ພວກເຮົາສັງເກດເຫັນວ່າການນຳໃຊ້ວິສາຫະກິດຈຳນວນ
  ຫຼາຍແມ່ນໄດ້ຮັບການຈັດການໂດຍເບິ່ງແຍງລະບົບ ທີ່ບໍ່ໄດ້ປົກປ້ອງບັນຊີຂອງຕົນເອງກັບ
  MFA. ເນື່ອງຈາກຜູ້ເບິ່ງແຍງລະບົບ ແມ່ນເປົ້າໝາຍທີ່ມີມູນຄ່າສູງ,
  ຜະລິດຕະພັນຈຶ່ງຄວນບໍ່ໃຊ້ MFA ແທນທີ່ຈະເລືອກເຂົ້າຮ່ວມ. ນອກຈາກນັ້ນ,
  ລະບົບຄວນແຈ້ງໃຫ້ຜູ້ເບິ່ງແຍງລະບົບລົງທະບຽນໃນ MFA
  ຢ່າງສະໝ່ຳສະເໝີຈົນກ່ວາພວກເຂົາໄດ້ເປີດໃຊ້ງານຢູ່ໃນບັນຊີຂອງພວກເຂົາຢ່າງສຳເລັດຜົນ
  NCSC ຂອງປະເທດເນເທີແລນດ໌ມີແນວທາງທີ່ຄ້າຍຄືກັບ CISA,
  ຈົ່ງເຂົ້າໄປເບິ່ງຂໍ້ມູນການຮັບຮອງຄວາມຖືກຕ້ອງຕາມຜູ້ໃໝ່ ເພື່ອເບິ່ງ ຂໍ້ມູນເພີ່ມເຕີມ ທີ່
  Mature Authentication Factsheet.

- ການລົງຊື່ພຽງເທື່ອດຽວ (SSO): ແອັບພລິເຄຊັນດ້ານໄອທີ (IT)
  ຄວນໃຊ້ເຕັກໂນໂລຢີການລົງຊື່ພຽງເທື່ອດຽວຜ່ານ. ມາດຕະຖານເປີດທີ່ທັນສະໄໝ. ຕົວຢ່າງເຊັ່ນ:
  ພາສາມາກອັບເພື່ອຢືນຢັນຄວາມປອດໄພ(SAML) ຫຼື ການເຊື່ອຕໍ່ID ແບບເປີດ(ODC.)
  ຄວາມສາມາດນີ້ຄວນມີໃຫ້ໃຊ້ໄດ້ຕາມຄ່າເລີ່ມຕົ້ນໂດຍບໍ່ມີຄ່າໃຊ້ ຈ່າຍເພີ່ມເຕີມ.
- ການບັນທຶກທີ່ປອດໄພ:
  ຈັດກຽມບັນທຶກການກວດສອບຄຸນນະພາບສູງໃຫ້ແກ່ລູກຄ້າໂດຍບໍ່ມີຄ່າໃຊ້ຈ່າຍເພີ່ມເຕີມ.
  ບັນທຶກການກວດສອບແມ່ນມີສຳຄັນສຳລັບການກວດສອບ ແລະ
  ຍົກລະດັບເຫດການດ້ານຄວາມປອດໄພທີ່ອາດເກີດຂຶ້ນໄດ້.
  ນອກຈາກນີ້ຍັງມີຄວາມສຳຄັນໃນລະຫວ່າງການສືບສວນກ່ຽວກັບເຫດການດ້ານຄວາມປອດໄພທີ່ຕ້ອງສົງໃສ
  ຫຼື ໄດ້ຮັບການຢືນຢັນ. ພິຈາລະນາແນວທາງປະຕິບັດທີ່ດີທີ່ສຸດເຊັ່ນ
  ການເຊື່ອມໂຍງເຂົ້າກັບຂໍ້ມູນຄວາມປອດໄພ ແລະ ລະບົບການຈັດການເຫດການ (SIEM)
  ທີ່ມີການໂຕ້ຕອບການຂຽນໂປລແກລມແອັບພລິເຄຊັນ (API) ທີ່ໃຊ້ເວລາສາກົນ (UTC),
  ການຈັດຮູບແບບເຂດເວລາມາດຕະຖານ ແລະເຕັກນິກການຈັດທຳເອກະສານທີ່ມີປະສິດທິພາບ.
- ໂປຣໄຟລ໌ການອະນຸຍາດຊອັບແວ:
  ຜູ້ສະໜອງຊອັບແວຄວນໃຫ້ຄຳແນະນຳກ່ຽວກັບບົດບາດຂອງໂປຣໄຟລ໌ທີ່ໄດ້ຮັບອະນຸຍາດ ແລະ
  ກໍລະນີການນຳໃຊ້ທີ່ກຳນົດໄວ້.
  ຜູ້ຜະລິດຄວນລວມຄຳເຕືອນທີ່ເຫັນໄດ້ຊັດເຈນທີ່ແຈ້ງເຕືອນໃຫ້ລູກຄ້າຮັບຮູ້ກ່ຽວກັບຄວາມສ່ຽງທີ່ເພີ່ມຂຶ້ນ
  ຖ້າພວກເຂົາບ່ຽງອອກໄປຈາກການອະນຸຍາດຂອງໂປຣໄຟລ໌ທີ່ແນະນຳ. ຕົວຢ່າງເຊັ່ນ:
  ທ່ານໜ່ວຍງານສາມາດເບິ່ງບັນທຶກຄົນເຈັບທັງໝົດໄດ້,

ແຕ່ຜູ້ກຳນົດເວລາທາງການແພດມີຂໍ້ຈຳກັດໃນການເຂົ້າເຖິງຂໍ້ມູນທີ່ຈຳເປັນສຳລັບການຈັດກຳນົດການນັດໝາຍ.

- ການຮັກສາຄວາມປອດໄພແບບຄາດຄະເນລ່ວງໜ້າຕໍ່ກັບຄວາມເຂົ້າກັນໄດ້ແບບຍ້ອນຫຼັງ: ເລື້ອຍໆເກີນໄປ, ທີ່ມີການຄວບຄຸມຄຸນສົມບັດແບບເກົ່າທີ່ເຂົ້າກັນໄດ້ແບບຍ້ອນຫຼັງ ແລະ ເປີດໃຊ້ເລື້ອຍໆຢູ່ໃນຜະລິດຕະພັນ ເຖິງວ່າຈະມີຄວາມສ່ຽງຕໍ່ຄວາມປອດໄພຂອງຜະລິດຕະພັນ.
  ຈັດລຳດັບຂອງການຮັກສາຄວາມປອດໄພຫຼາຍກວ່າຄວາມເຂົ້າກັນໄດ້ແບບຍ້ອນຫຼັງ,
  ຊ່ວຍໃຫ້ທີມງານຮັກສາຄວາມປອດໄພສາມາດລົບຄຸນສົມບັດທີ່ບໍ່ປອດໄພອອກໄດ້ເຖິງແມ່ນວ່າມັນຈະເຮັດໃຫ້ເກີດການປ່ຽນແປງທີ່ເສັຍຫາຍກໍຕາມ.
- ຕິດຕາມ ແລະ ຫຸດຂະໜາດ “ຄູ່ມືຄວບຄຸມການຊຸບແຂງ”: ຫຸດຂະໜາດຂອງ “ຄູ່ມືຄວບຄຸມການຊຸບແຂງ” ທີ່ຜະລິດສຳລັບຜະລິດຕະພັນ ແລະ
  ພະຍາຍາມຮັບປະກັນວ່າຂະໜາດຈະຫຼຸດລົງເມື່ອເວລາຜ່ານໄປເມື່ອມີການເປີດຕົວຊຸບແຂລຸ້ນໃໝ່.
  ລວມສ່ວນປະກອບຂອງ " ຄູ່ມືຄວບຄຸມການຊຸບແຂງ" ເປັນການຕັ້ງຄ່າເລີ່ມຕົ້ນຂອງຜະລິດຕະພັນ.
  ໜ່ວຍງານຜູ້ຂຽນຮັບຮູ້ວ່າ
  ຄູ່ມືຄວບຄຸມການຊຸບແຂງທີ່ສັ້ນລົງເປັນຜົນມາຈາກການຮ່ວມມືຢ່າງຕໍ່ເນື່ອງກັບລູກຄ້າທີ່ມີຢູ່ ແລະ ລວມທັງຄວາມພະຍາຍາມຂອງທີມງານຜະລິດຕະພັນຈຳນວນຫຼາຍ, ລວມທັງປະສົບການຂອງຜູ້ໃຊ້ (UX) ອີກດ້ວຍ.
- ພິຈາລະນາປະສົບການຂອງຜູ້ໃຊ້ທີ່ຕາມມາຂອງການຕັ້ງຄ່າຄວາມປອດໄພ:
  ແຕ່ລະການຕັ້ງຄ່າໃໝ່ຈະເພີ່ມພາລະທາງດ້ານຄວາມຄິດໃຫ້ກັບຜູ້ໃຊ້ປາຍທາງ ແລະ
  ຄວນໄດ້ຮັບປະເມີນຮ່ວມກັບຜົນປະໂຫຍດທາງທຸລະກິດທີ່ໄດ້ຮັບ. ຕາມຫລັກການແລ້ວ,
  ບໍ່ຄວນມີການຕັ້ງຄ່າ;
  ຄວນລວມການຕັ້ງຄ່າທີ່ປອດໄພທີ່ສຸດຄວນເຂົ້າໃນຜະລິດຕະພັນຕາມຄ່າເລີ່ມຕົ້ນແທນ.
  ເມື່ອຈຳເປັນຕ້ອງກຳນົດຄ່າ,
  ໂຕເລືອກເລີ່ມຕົ້ນຄວນຈະມີຄວາມປອດໄພຢ່າງກວ້າງຂວາງຕໍ່ກັບໄພຂົ່ມຂູ່ທົ່ວໄປ.

ໜ່ວຍງານຜູ້ຂຽນຮັບຮູ້ວ່າການປ່ຽນແປງເຫຼົ່ານີ້ອາດຈະມີຜົນກະທົບດ້ານການດຳເນີນງານກ່ຽວກັບວິທີການເຮັດວຽກຂອງຊຸບແຂ. ດັ່ງນັ້ນ,
ການປ້ອນຂໍ້ມູນຂອງລູກຄ້າແມ່ນມີຄວາມສຳຄັນໃນການສ້າງຄວາມດຸ່ນດ່ຽງລະຫວ່າງການພິຈາລະນາດ້ານການດຳເນີນງານ ແລະ ຄວາມປອດໄພ. ໜ່ວຍງານຜູ້ຂຽນເຊື່ອວ່າການພັດທະນາແຜນງານທີ່ເປັນລາຍລັກອັກສອນ ແລະ ການສະໜັບສະໜູນຜູ້ບໍລິຫານທີ່ຈັດລຳດັບຄວາມສຳຄັນຂອງແນວຄວາມຄິດເຫຼົ່ານີ້ເຂົ້າໄປໃນຜະລິດຕະພັນທີ່ສຳຄັນຂອງອົງກອນແມ່ນບາດກ້າວທຳອິດທີ່ຈະຫັນປ່ຽນໄປສູ່ການປະຕິບັດໃນການພັດທະນາຊຸບແຂທີ່ປອດໄພ.
ໃນຂະນະທີ່ການປ້ອນຂໍ້ມູນຂອງລູກຄ້າມີຄວາມສຳຄັນ,

ໜ່ວຍງານຜູ້ຂຽນໄດ້ສັງເກດເຫັນກໍລະນີສຳຄັນທີ່ລູກຄ້າບໍ່ເຕັມໃຈ ຫຼື
ບໍ່ສາມາດຮັບຮອງເອົາມາດຕະຖານທີ່ໄດ້ຮັບການປັບປຸງມາໃຊ້ ຊຶ່ງມັກຈະເປັນໂປຣໂຕຄອນເຄືອຂ່າຍ.
ເປັນສິ່ງສຳຄັນສຳລັບຜູ້ຜະລິດທີ່ຈະສ້າງແຮງຈູງໃຈທີ່ມີຄວາມໝາຍສຳລັບລູກຄ້າທີ່ຈະຕິດຕາມຂ່າວສານປັດຈຸບັນ
ແລະ ບໍ່ປ່ອຍໃຫ້ພວກເຂົາຢູ່ໃນພາວະອ່ອນແອຕະຫຼອດໄປ.

ຄູ່ມື ການແຂງຕົວ ແລະ ການຄາຍຕົວ

ຄູ່ມືການເຮັດໃຫ້ແຂງອາດຈະເປັນຜົນມາຈາກການຂາດການຄວບຄຸມຄວາມປອດໄພຂອງຜະລິດຕະພັນຝັງຢູ່ໃນສ
ະຖາປັດຕະຍະກຳຂອງຜະລິດຕະພັນຕັ້ງແຕ່ເລີ່ມຕົ້ນພັດທະນາ. ດັ່ງນັ້ນ,
ຄຳແນະນຳທີ່ເຂັ້ມງວດຍັງສາມາດເປັນແຜນງານສຳລັບຝ່າຍກົງກັນຂ້າມເພື່ອລະບຸ ແລະ
ໃຊ້ປະໂຫຍດຈາກຄຸນສົມບັດທີ່ບໍ່ປອດໄພ. ເປັນເລື່ອງປົກກະຕິສຳລັບຫຼາຍໆອົງກອນ
ຈະບໍ່ຮູ້ຈັກຄູ່ມືຄວບຄຸມການລຸບແຂງ, ດັ່ງນັ້ນພວກເຂົາຈຶ່ງປ່ອຍໃຫ້ການຕັ້ງຄ່າອຸປະກອນຢູ່ໃນທ່າທາງທີ່ບໍ່ປອດໄພ.
ຮູບແບບນີ້ຄ້າຍກັບທີ່ຮູ້ຈັກເປັນຄູ່ມືການຄາຍຄອນແທນທີ່ຄູ່ມືຄວບຄຸມການລຸບແຂງດັ່ງກ່າວ ແລະ
ອະທິບາຍວ່າຜູ້ໃຊ້ຄວນເຮັດການປ່ຽນແປງໃດໃນຂະນະດຽວກັນກໍບອກຄວາມສ່ຽງດ້ານຄວາມປອດໄພທີ່ຕາມມາອີ
ກດ້ວຍ.
ແທນທີ່ຈະພັດທະນາຄູ່ມືຄວບຄຸມການລຸບແຂງທີ່ມີລາຍການວິທີການຮັກສາຄວາມປອດໄພຜະລິດຕະພັນ,
ໜ່ວຍງານຜູ້ຂຽນແນະນຳໃຫ້ຜູ້ຜະລິດຊອັບແວປ່ຽນໄປສູ່ວິທີຄວາມປອດໄພໂດຍຄ່າເລີ່ມຕົ້ນ
ໂດຍການຈັດທຳຄູ່ມືການຄາຍຕົວ
ຄູ່ມືເຫຼົ່ານີ້ອະທິບາຍເຖິງຄວາມສ່ຽງທາງທຸລະກິດຂອງການຕັດສິນໃຈໃນພາສາທີ່ເຂົ້າໃຈໄດ້ງ່າຍ ແລະ
ສາມາດສ້າງຄວາມຮັບຮູ້ຂອງອົງກອນກ່ຽວກັບຄວາມສ່ຽງຕ່ຳການໂຈມຕີທາງໄຊເບີທີ່ເປັນອັນຕະລາຍ.
ການແລກປ່ຽນດ້ານຄວາມປອດໄພຄວນຈະຖືກກຳນົດໂດຍຜູ້ບໍລິຫານລະດັບສູງຂອງລູກຄ້າ
ໂດຍສ້າງຄວາມດຸ່ນດ່ຽງລະຫວ່າງຄວາມປອດໄພກັບຂໍ້ກຳນົດທຸລະກິດອື່ນໆ.

ຄຳແນະນຳສຳລັບລູກຄ້າ

ໜ່ວຍງານຜູ້ຂຽນແນະນຳອົງກອນໃຫ້ຜູ້ຜະລິດຕັກໂນໂລຍີທີ່ໃຫ້ການສະໜອງຂອງຕົນຮັບຜິດຊອບຕໍ່ຜົນໄດ້ຮັບ
ດ້ານຄວາມປອດໄພຂອງຜະລິດຕະພັນຂອງຕົນ. ໃນສ່ວນໜຶ່ງຂອງສິ່ງນີ້
ໜ່ວຍງານຜູ້ຂຽນແນະນຳໃຫ້ຜູ້ບໍລິຫານຂອງອົງກອນຈັດລຳດັບຄວາມສຳຄັນຂອງການຊື້ຜະລິດຕະພັນຄວາມປອ
ດໄພໂດຍການອອກແບບ ແລະ ຄວາມປອດໄພໂດຍຄ່າເລີ່ມຕົ້ນ.
ສິ່ງນີ້ສາມາດສະແດງອອກມາໂດຍຜ່ານການສ້າງນະໂຍບາຍທີ່ຮຽກຮ້ອງໃຫ້ພະແນກໄອທີ (IT)
ຕ້ອງປະເມີນຄວາມປອດໄພຂອງຊອັບແວຂອງຜູ້ຜະລິດກ່ອນທີ່ຈະຊື້ ລວມທັງໃຫ້ອຳນາດພະແນກໄອທີ (IT)
ທີ່ຈະຍົກເລີກຖ້າຈຳເປັນ.

ພະແນກໄອທີ (IT)
ຄວນໄດ້ຮັບສິດອຳນາດໃນການພັດທະນາເງື່ອນໄຂການຊື້ທີ່ເນັ້ນໜັກເຖິງຄວາມສຳຄັນຂອງຫຼັກປະຕິບັດຄວາມປອດໄພໂດຍການອອກແບບ ແລະ ຄວາມປອດໄພໂດຍຄ່າເລີ້ມຕົ້ນ(ທັງສອງທີ່ລະບຸໄວ້ໃນເອກະສານນີ້ ແລະ ອື່ນໆທີ່ພັດທະນາໂດຍອົງກອນ). ນອກຈາກນັ້ນ, ພະແນກໄອທີ (IT)
ຄວນໄດ້ຮັບການສະໜັບສະໜູນຈາກຝ່າຍບໍລິຫານໃນເວລາທີ່ບັງຄັບໃຊ້ເງື່ອນໄຂເຫຼົ່ານີ້ໃນການຕັດສິນໃຈຊື້. ການຕັດສິນໃຈຂອງອົງກອນເພື່ອຍອມຮັບຄວາມສ່ຽງທີ່ກ່ຽວຂ້ອງກັບຜະລິດຕະພັນເຕັກໂນໂລຢີສະເພາະຄວນໄດ້ຮັບການບັນທຶກ
ຢ່າງເປັນທາງການ, ໄດ້ຮັບການອະນຸມັດໂດຍຜູ້ບໍລິຫານທຸລະກິດລະດັບສູງຂອງທຸລະກິດ ແລະ ນຳສະເໜີຕໍ່ຄະນະກຳມະການບໍລິຫານເປັນປະຈຳ.
ການບໍລິການໄອທີ (IT)
ທີ່ສຳຄັນຂອງອົງກອນທີ່ສຳຄັນທີ່ສະໜັບສະໜູນທ່າທາງການຮັກສາຄວາມປອດໄພຂອງອົງກອນ ເຊັ່ນ ເຄືອຂ່າຍຂອງອົງກອນ ການຈັດການຂໍ້ມູນປະຈຳຕົວ ແລະ ການເຂົ້າເຖິງ ແລະ
ການດຳເນີນການດ້ານຄວາມປອດໄພ ແລະ
ຄວາມສາມາດໃນການສະຕອບສະໜອງຄວນຈະໄດ້ຮັບການເຫັນວ່າເປັນໜ້າທີ່ທາງທຸລະກິດທີ່ສຳຄັນທີ່ໄດ້ຮັບທຶນສະໜັບສະໜູນເພື່ອໃຫ້ສອດຄ່ອງກັບຄວາມສຳຄັນຕໍ່ຜົນສຳເລັດຂອງພາລະກິດຂອງອົງກອນ.
ອົງກອນຄວນພັດທະນາແຜນເພື່ອຍົກລະດັບຄວາມສາມາດເຫຼົ່ານີ້ເພື່ອໃຊ້ປະໂຫຍດຈາກຜູ້ຜະລິດທີ່ຍອມຮັບການປະຕິບັດຄວາມປອດໄພໂດຍການອອກແບບ ແລະຄວາມປອດໄພໂດຍຄ່າເລີ່ມຕົ້ນ.
ຖ້າເປັນໄປໄດ້, ອົງກອນຄວນພະຍາຍາມສ້າງການພົວພັນແບບຄູ່ຮ່ວມມືຍຸດທະສາດກັບ
ຜູ້ສະໜອງດ້ານໄອທີທີ່ສຳຄັນຂອງພວກເຂົາ.
ສາຍພົວພັນດັ່ງກ່າວປະກອບມີຄວາມໂອ້ອ້ວງໃຈໃນຫຼາຍລະດັບຂອງອົງກອນ ແລະ
ຈັດຫາຍານພາຫະນະເພື່ອແກ້ໄຂບັນຫາ ແລະ ລະບຸລຳດັບຄວາມສຳຄັນຮ່ວມກັນ.
ການຮັກສາຄວາມປອດໄພຄວນຈະເປັນອົງປະກອບທີ່ສຳຄັນຂອງການພົວພັນດັ່ງກ່າວ ແລະ
ອົງກອນຄວນພະຍາຍາມເນັ້ນເຖິງຄວາມສຳຄັນຂອງຫຼັກປະຕິບັດຄວາມປອດໄພໂດຍການອອກແບບ ແລະ ຄວາມປອດໄພໂດຍຄ່າເລີ່ມຕົ້ນໃນທັງສອງຢ່າງເປັນທາງການ (ເຊັ່ນ: ສັນຍາ ຫຼື ຕົກລົງຜູ້ຂາຍ) ແລະ
ທີ່ບໍ່ເປັນທາງການຂອງຄວາມສຳພັນ.
ອົງກອນຄວນຄາດຫວັງຄວາມໂປ່ງໃສຈາກຜູ້ສະໜອງດ້ານເຕັກໂນໂລຢີຂອງຕົນກ່ຽວກັບແນວທາງການຄວບຄຸມພາຍໃນຂອງພວກເຂົາຕະຫຼອດຈົນແຜນການເຮັດວຽກ ໄປສູ່ການຮັບຮອງເອົາຫຼັກປະຕິບັດ
ຄວາມປອດໄພໂດຍການອອກແບບ ແລະ ຄວາມປອດໄພໂດຍຄ່າເລີ່ມຕົ້ນ.
ນອກເໜືອຈາກການເຮັດໃຫ້ຄວາມປອດໄພໂດຍຄ່າເລີ່ມຕົ້ນ ມີຄວາມສຳຄັນພາຍໃນອົງກອນແລ້ວ, ຜູ້ນຳດ້ານໄອທີຄວນຮ່ວມມືກັບເພື່ອນຮ່ວມງານໃນອຸດສາຫະກຳຂອງຕົນເພື່ອໃຫ້ເຂົ້າໃຈວ່າຜະລິດຕະພັນ ແລະ

ການບໍລິການໃດທີ່ລວມເອົາຫຼັກການການອອກແບບເຫຼົ່ານີ້ໄດ້ດີທີ່ສຸດ.
ຜູ້ນໍາເຫຼົ່ານີ້ຄວນປະສານງານການຮ້ອງຂໍຂອງພວກເຂົາເພື່ອຊ່ວຍໃຫ້ຜູ້ຜະລິດຈັດລໍາດັບຄວາມສໍາຄັນຂອງຄວາມຄິດລິເລີ່ມດ້ານຄວາມປອດໄພທີ່ຈະເກີດຂຶ້ນ. ໂດຍການເຮັດວຽກຮ່ວມກັນ
ລູກຄ້າສາມາດຊ່ວຍສະໜອງການບ້ອນຂໍ້ມູນທີ່ມີຄວາມໝາຍໃຫ້ກັບຜູ້ຜະລິດ ແລະ
ສ້າງແຮງຈູງໃຈໃຫ້ພວກເຂົາຈັດລໍາດັບຄວາມສໍາຄັນດ້ານຄວາມປອດໄພ.
ເມື່ອນໍາໃຊ້ປະໂຫຍດຈາກລະບົບຄລາວດ໌,
ອົງກອນຄວນກວດສອບໃຫ້ແນ່ໃຈວ່າພວກເຂົາເຂົ້າໃຈຮູບແບບຄວາມຮັບຜິດຊອບຮ່ວມກັນກັບຜູ້ສະໜອງເຕັກໂນໂລຢີຂອງຕົນ. ນັ້ນຄື
ອົງກອນຄວນມີຄວາມຊັດເຈນກ່ຽວກັບຄວາມຮັບຜິດຊອບຮ່ວມກັນດ້ານຄວາມປອດໄພຂອງຜູ້ສະໜອງຫຼາຍກວ່າຄວາມຮັບຜິດຊອບຂອງລູກຄ້າ

ອົງກອນຄວນຈັດລໍາດັບຄວາມສໍາຄັນຂອງຜູ້ໃຫ້ບໍລິການລະບົບຄລາວດ໌ທີ່ມີຄວາມໂປ່ງໃສກ່ຽວກັບທ່າທາງການຮັກສາຄວາມປອດໄພ, ການຄວບຄຸມພາຍໃນ ແລະ
ຄວາມສາມາດໃນການປະຕິບັດຕາມພາລະໜ້າທີ່ຂອງຕົນພາຍໃຕ້ຮູບແບບຄວາມຮັບຜິດຊອບຮ່ວມກັນ.

ຂໍ້ຈໍາກັດຄວາມຮັບຜິດຊອບ

ຂໍ້ມູນໃນບົດລາຍງານນີ້ແມ່ນມີໃຫ້ "ຕາມທີ່ເປັນ" ເພື່ອຈຸດປະສົງໃນການໃຫ້ຂໍ້ມູນຂ່າວສານເທົ່ານັ້ນ. CISA, ແລະ ໜ່ວຍງານຜູ້ຂຽນບໍ່ໄດ້ຮັບຮອງຜະລິດຕະພັນການຄ້າ ຫຼື ການບໍລິການ, ລວມທັງຫົວຂໍ້ການວິເຄາະໃດໆ.
ການອ້າງອີງເຖິງຫົວໜ່ວຍການຄ້າສະເພາະເຈາະຈົງ ຫຼື ຜະລິດຕະພັນທາງການຄ້າ, ຂະບວນການ ຫຼື
ການບໍລິການໂດຍເຄື່ອງໝາຍການບໍລິການ, ເຄື່ອງໝາຍການຄ້າ, ຜູ້ຜະລິດ ຫຼື ອື່ນໆ, ບໍ່ໄດ້ປະກອບ ຫຼື
ໝາຍເຖິງການຮັບຮອງ, ການແນະນໍາ ຫຼື ການຫຼີ້ມພັກພວກ ໂດຍ CISA ແລະ ອົງການຜູ້ຂຽນ.
ເອກະສານນີ້ແມ່ນຄວາມຄິດລິເລີ່ມຮ່ວມກັນໂດຍ CISA
ຊຶ່ງບໍ່ໄດ້ເຮັດໜ້າທີ່ເປັນເອກະສານລະບຽບການໂດຍອັດຕະໂນມັດ.

ແຫຼ່ງຂໍ້ມູນ

CISA

- CISA’s SBOM Guidance
- CISA’s Cross-Sector Cybersecurity Performance Goals
- Guidelines on Technology Interoperability

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

NSA

- NSA's Cybersecurity Information Sheet on Memory Safety
- NSA's ESF Securing the Software Supply Chain: Best Practices for Suppliers

FBI

- Understanding and Responding to the SolarWinds Supply Chain Attack: The Federal Perspective
- The Cyber Threat - Response and Reporting
- FBI's Cyber Strategy

ສະຖາບັນມາດຕະຖານ ແລະ ເຕັກໂນໂລຊີ ແຫ່ງຊາດ (National Institute of Standards and Technology (NIST))

- NIST's Digital Identity Guidelines
- NIST's Cyber Security Framework
- NIST's Secure Software Development Framework (SSDF)

ສູນຄວາມປອດໄພທາງໄຊເບີ ຂອງ ອອສເຕຣລ໌ (Australian Cyber Security Centre (ACSC))

- ACSC's IoT Code of Practice Guidance for Manufacturers

ສູນຄວາມປອດໄພທາງໄຊເບີແຫ່ງຊາດຂອງສະຫະຣາຊອານາຈັກ

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

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

ສູນຄວາມປອດໄພ ທາງ ໄຊເບີ ຂອງ ການາດາ (Canadian Centre for Cyber Security (CCS))

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

ຫ້ອງການລັດຖະບານກາງເພື່ອຄວາມປອດໄພຂໍ້ມູນຂ່າວສານ ຂອງ ເຢັຍຣະມັນ (Germany's Federal Office for Information Security (BSI))

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

ສູນ Netherlands' National Cyber Security Centre

- NCSC-NL's Mature Authentication Factsheet
- How Complex Systems Fail
- The New Look in complex system failure

ອື່ນໆ

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