TLP:CLEAR

ຄວາມປອດໄພໂດຍ ການອອກແບບ

ການປ່ຽນຄວາມດຸນດ່ຽງ ຄວາມສ່ຽງດ້ານຄວາມປອດໄພທາງໄຊເບີ:

ຫຼັກການ ແລະ ວິທີການສຳລັບ
ຄວາມປອດໄພໂດຍອອກແບບຊອັບແວ

TLP:CLEAR

Communications Security Establishment

Canadian Centre for Cyber Security

Centre de la sécurité des télécommunications

Centre canadien pour la cybersécurité

ສາລະບານ

ພາບລວມ: ຄວາມສ່ຽງໂດຍການອອກແບບ

ເທັກໂນໂລຍີຖືກລວມເຂົ້າໃນເກືອບທຸກດ້ານຂອງຊີວິດປະຈຳວັນ ເນື່ອງຈາກລະບົບການ ທີ່ເຊື່ອມຕໍ່ກັບອິນເຕີເນັດໄດ້ເຊື່ອມໂຍງພວກເຮົາເຂົ້າກັບ ລະບົບທີ່ສຳຄັນທີ່ສົ່ງຜົນກະທົບໂດຍກົງຕໍ່ຄວາມຈະເລີນຮຸ່ງເຮືອງທາງດ້ານເສດຖະກິດ, ຊີວິດການເປັນຢູ່ ແລະ ແມ່ນແຕ່ສຸຂະພາບ ຂອງພວກ ເຮົາ ຕັ້ງແຕ່ການຄຸ້ມຄອງຂໍ້ມູນສ່ວນຕົວຈົນເຖິງ ການດູແລທາງການແພດ. ຕົວຢ່າງໜຶ່ງຂອງຂໍ້ເສຍຂອງຄວາມສະດວກສະບາຍດັ່ງກ່າວແມ່ນ ການລະເມີດທາງໄຊເບີ ທົ່ວໂລກທີ່ສົ່ງຜົນໃຫ້ໂຮງໝໍຕ້ອງຍົກເລີກການຜ່າຕັດ ແລະ ຫັນປ່ຽນການດູແລຄົນເຈັບ. ເທັກໂນໂລຍີທີ່ບໍ່ປອດໄພ ແລະ ຊ່ອງໂຫວ່ໃນລະບົບທີ່ສຳຄັນອາດຈະພາໃຫ້ມີການບຸກລຸກ ທາງໄຊເບີທີ່ເປັນອັນຕະລາຍຊຶ່ງນຳໄປສູ່ຄວາມສ່ຽງດ້ານຄວາມປອດໄພ[1].

ດັ່ງນັ້ນ, ມັນຈຶ່ງເປັນສິ່ງສຳຄັນສຳລັບຜູ້ຜະລິດຊອັບແວທີ່ຈະຕ້ອງຮັກສາຄວາມປອດໄພ ໂດຍການອອກແບບ ແລະ ຮັກສາຄວາມປອດໄພ ໂດຍຄ່າເລີ່ມຕົ້ນຂອງຈຸດປະສານງານຂອງຂະບວນການອອກແບບ ແລະ ການພັດທະນາຜະລິດຕະພັນ. ຜູ້ຈຳໜ່າຍບາງຄົນມີຄວາມກ້າວໜ້າ ຢ່າງຫຼວງຫຼາຍໃນການຂັບເຄື່ອນອຸດສາຫະກຳໄປທາງໜ້າໄປໃນຂ້າງໜ້າໃນດ້ານການຮັບປະກັນຊອັບແວໃນຂະນະທີ່ຄົນອື່ນຍັງຄົງຕາມຫຼັງ ຢູ່. ອົງກອນຜູ້ຂຽນຊຸກຍູ້ໃຫ້ຜູ້ຜະລິດເທັກໂນໂລຍີທຸກຄົນສ້າງຜະລິດຕະພັນຂອງຕົນໂດຍ ອີງໃສ່ການຫຼຸດຜ່ອນພາລະຂອງຄວາມປອດໄພ ທາງໄຊເບີໃຫ້ກັບລູກຄ້າ ລວມທັງການປ້ອງກັນບໍ່ໃຫ້ເຂົາເຈົ້າຕ້ອງ ດຳເນີນການຕິດຕາມ, ການອັບເດດເປັນປົກກະຕິ ແລະ ການຄວບຄຸມ ຄວາມເສຍຫາຍໃນລະບົບຂອງຕົນຢ່າງຕໍ່ເນື່ອງເພື່ອຫຼຸດຜ່ອນການບຸກລຸກທາງໄຊເບີ. ນອກຈາກນີ້ ພວກເຮົາຍັງສະໜັບສະໜູນໃຫ້ຜູ້ຜະລິດ ຊອັບແວສ້າງຜະລິດຕະພັນຂອງຕົນໃນລັກສະນະ ທີ່ອຳນວຍຄວາມສະດວກໃນການຕັ້ງຄ່າ ການຕິດຕາມເບິ່ງ ແລະ ການອັບເດດຕາມປົກກະຕິ ໂດຍອັດຕະໂນມັດ. ຜູ້ຜະລິດໄດ້ຮັບການຊຸກຍູ້ໃຫ້ເປັນເຈົ້າຂອງໃນການປັບປຸງຜົນໄດ້ຮັບດ້ານຄວາມປອດໄພ ຂອງລູກຄ້າ. ໃນອາດີດ, ຜູ້ຜະ ລິດຊອັບແວໄດ້ອີງໃສ່ການແກ້ໄຂຊ່ອງໂຫ່ວທີ່ພົບເຫັນຫຼັງຈາກລູກຄ້າໄດ້ນຳໃຊ້ຜະລິດຕະພັນແລ້ວ, ໂດຍກຳນົດໃຫ້ລູກຄ້າຕ້ອງຕິດຕັ້ງ ແພັຊ (patches) ເຫຼົ່ານັ້ນດ້ວຍຄ່າໃຊ້ຈ່າຍຂອງຕົນເອງ. ໂດຍການລວມເອົາຄວາມປອດໄພໂດຍຫຼັກປະຕິບັດໃນການອອກແບບເທົ່ານັ້ນທີ່ພວກເຮົາ ຈະທຳລາຍວົງຈອນອັນໂຫດຮ້າຍຂອງການສ້າງ ແລະ ນຳໃຊ້ການແກ້ໄຂຢ່າງຕໍ່ເນື່ອງໄດ້. **ໝາຍເຫດ:** ຄຳວ່າ "ຄວາມປອດໄພໂດຍການອອກແບບ" ກວມເອົາທັງຄວາມປອດໄພ ໂດຍ ການອອກແບບ ແລະ ການຮັກສາຄວາມປອດໄພໂດຍຄ່າເລີ່ມຕົ້ນ.

ເພື່ອໃຫ້ບັນລຸມາດຕະຖານຄວາມປອດໄພຂອງຊອັບແວລະດັບສູງນີ້ ອົງກອນຜູ້ຂຽນ ໄດ້ຊຸກຍູ້ ໃຫ້ຜູ້ຜະລິດຈັດລຳດັບຄວາມສຳຄັນຂອງ ການເຊື່ອມໂຍງຂອງຄວາມປອດໄພຂອງ ຜະລິດ ຕະພັນເປັນຂໍ້ກຳນົດເບື້ອງຕົ້ນທີ່ສຳຄັນຕໍ່ຄຸນສົມບັດ ແລະ ຄວາມໄວໃນການອອກສູ່ຕະຫຼາດ. ເມື່ອເວລາຜ່ານໄປ, ທີມງານວິສະວະກຳຈະສາມາດສ້າງຈັງຫວະໃນສະພາວະຄົງທີ່ແບບໃໝ່ ໄດ້ໂດຍການຮັກສາຄວາມປອດໄພໄດ້ຮັບການ ອອກແບບຢ່າງແທ້ຈິງ ແລະ ໃຊ້ຄວາມພະຍາ ຍາມໜ້ອຍລົງໃນການຮັກສາ.

ເພື່ອສະທ້ອນໃຫ້ເຫັນມຸມມອງນີ້, ສະຫະພາບເອີຣົບໄດ້ເນັ້ນຢ້ຳເຖິງຄວາມສຳຄັນຂອງ ຄວາມປອດໄພຂອງຜະລິດຕະພັນໃນ ກົດໝາຍວ່າດ້ວຍ ຄວາມສາມາດໃນການຟື້ນຕົວທາງໄຊເບີ, ໂດຍເນັ້ນໜັກວ່າຜູ້ຜະລິດຄວນໃຊ້ຄວາມປອດໄພຕະຫຼອດວົງຈອນຊີວິດ ຂອງ ຜະລິດຕະພັນເພື່ອ ປ້ອງກັນຜູ້ຜະລິດຈາກການແນະນຳຜະລິດຕະພັນທີ່ມີຄວາມສ່ຽງ ເຂົ້າສູ່ຕະຫຼາດ.

[1] ອົງກອນຜູ້ຂຽນຮັບຮູ້ວ່າຄຳວ່າ "ຄວາມປອດໄພ" ມີຄວາມໝາຍຫຼາຍຢ່າງຂຶ້ນກັບບໍລິບົດທີ່ໃຊ້. ສຳລັບຈຸດປະສົງຂອງຄູ່ມືນີ້, "ຄວາມປອດໄພ" ຈະໝາຍເຖິງການຍົກສູງມາດຕະຖານຄວາມປອດໄພດ້ານເທັກໂນໂລຍີເພື່ອປົກປ້ອງລູກຄ້າຈາກກິດຈະກຳທາງໄຊເບີທີ່ເປັນອັນຕະລາຍ.

ເພື່ອສ້າງອະນາຄົດທີ່ເທັກໂນໂລຢີ ແລະ ຜະລິດຕະພັນທີ່ກ່ຽວຂ້ອງມີຄວາມປອດໄພຫຼາຍຂຶ້ນສຳລັບລູກຄ້າ, ອົງກອນຜູ້ຂຽນຮຽກຮ້ອງໃຫ້ຜູ້ຜະລິດປັບປຸງໂປຣແກຣມການອອກແບບ ແລະ ການພັດທະນາຂອງຕົນເພື່ອອະນຸຍາດໃຫ້ມີການຈັດສົ່ງສິນຄ້າທີ່ ປອດໄພໂດຍການອອກແບບ ແລະ ຄ່າເລີ່ມຕົ້ນເທົ່ານັ້ນ. ກ່ອນການພັດທະນາ ຜະລິດຕະພັນທີ່ປອດໄພໂດຍການອອກແບບໄດ້ຮັບການອອກແບບໂດຍຄຳນຶງເຖິງຄວາມປອດໄພຂອງລູກຄ້າເປັນເປົ້າໝາຍທາງທຸລະກິດຫຼັກ ບໍ່ ພຽງແຕ່ຄຸນສົມບັດທາງ ດ້ານເທັກນິກເທົ່ານັ້ນ. ຜະລິດຕະພັນຄວາມປອດໄພໂດຍການອອກແບບ ເລີ່ມຕົ້ນດ້ວຍເປົ້າໝາຍນັ້ນກ່ອນທີ່ການພັດທະນາຈະເລີ່ມຕົ້ນ. ຜະລິດຕະພັນທີ່ມີຢູ່ແລ້ວສາມາດພັດທະນາໄປສູ່ຄວາມປອດໄພໂດຍການອອກແບບໂດຍ ສະຖານະການອອກແບບຜ່ານການເຮັດຊ້ຳຄືນຫຼາຍຄັ້ງ. ຜະລິດຕະພັນຄວາມປອດໄພໂດຍຄ່າເລີ່ມຕົ້ນແມ່ນຜະລິດຕະພັນທີ່ປອດໄພໃນການນຳໃຊ້ ທັນທີທີ່ເປີດກ່ອງ ໂດຍບໍ່ຈຳເປັນຕ້ອງມີການປ່ຽນແປງການຕັ້ງຄ່າເລັກນ້ອຍ ຫຼື ບໍ່ມີເລີຍ ແລະ ຄຸນນະສົມບັດດ້ານຄວາມປອດໄພທີ່ສາມາດໃຊ້ໄດ້ໂດຍບໍ່ມີຄ່າໃຊ້ຈ່າຍເພີ່ມເຕີມ. ປັດຊະຍາທັງສອງນີ້ຮ່ວມກັນຍົກຍ້າຍພາລະອັນຫຼວງຫຼາຍໃນການຮັກສາຄວາມປອດໄພ ໃຫ້ກັບຜູ້ຜະລິດ ແລະ ຫຼຸດຜ່ອນໂອກາດທີ່ລູກຄ້າຈະຕົກເປັນເຫຍື່ອຂອງເຫດການດ້ານຄວາມປອດໄພທີ່ເປັນຜົນມາຈາກການກຳນົດ ຄ່າທີ່ບໍ່ຖືກຕ້ອງ, ການແກ້ໄຂ ລູກຄ້າທີ່ວ່ອງໄວບໍ່ພຽງພໍ ຫຼື ບັນຫາທົ່ວໄປອື່ນໆອີກຫຼວງຫຼາຍ.

ໜ່ວຍງານຄວາມປອດໄພທາງໄຊເບີ ແລະ ໂຄງສ້າງພື້ນຖານ(CISA) ອົງການ ຄວາມປອດໄພແຫ່ງຊາດ (NSA), ສຳນັກງານສືບສວນຂອງລັດຖະບານກາງ (FBI) ແລະ ຄູ່ຮ່ວມງານສາກົນຕໍ່ໄປນີ້[2] ໃຫ້ຄຳແນະນຳໃນຄູ່ມືນີ້ເພື່ອເສັ້ນທາງ ສຳລັບ ຜູ້ຜະລິດ ຊອັບແວເພື່ອຮັບປະກັນຄວາມປອດໄພຂອງຜະລິດຕະພັນ ຂອງພວກເຂົາ:

- ສູນຄວາມປອດໄພທາງໄຊເບີຂອງອອັສເຕຣເລັຍ (ACSC)
- ສູນຄວາມປອດໄພທາງໄຊເບີຂອງການາດາ (CCCS)
- ສູນຄວາມປອດໄພທາງໄຊເບີແຫ່ງຊາດຂອງສະຫະຣາຊອານາຈັກ (NCSC-UK)
- ສຳນັກງານຄວາມປອດໄພຂໍ້ມູນຂ່າວສານຂອງເຢັຍຣະມັນ (BSI)
- ສູນຄວາມປອດໄພທາງໄຊເບີແຫ່ງຊາດຂອງເນເທີແລນດ໌ (NCSC-NL)
- ສູນຄວາມປອດໄພທາງໄຊເບີແຫ່ງຊາດຂອງນໍເວ (NCSC-NO)
- ທີມງານຕອບໂຕ້ສຸກເສີນດ້ານຄອມພິວເຕີນິວຊີແລນດ໌ (CERT NZ) ແລະ ສູນຄວາມປອດໄພທາງໄຊເບີແຫ່ງຊາດ ຂອງ ນິວຊີແລນດ໌ (NCSC-NZ).
- ໜ່ວຍງານອິນເຕີເນັດ ແລ ະ ຄວາມປອດໄພ ຂອງເກົາຫຼີ (KISA)
- ຄະນະກຳມະການ ໄຊເບີ ແຫ່ງຊາດ ຂອງ ອິດສະຣາເອລ (INCD)
- ສູນກຽມຄວາມພ້ອມດ້ານເຫດການ ແລະ ຍຸດທະສາດແຫ່ງຊາດຍີ່ປຸ່ນ ສຳລັບຄວາມປອດໄພທາງໄຊເບີ (NISC) ແລະ ສູນ ປະສານງານທີມງານ ຕອບໂຕ້ເຫດສຸກເສີນທາງຄອມພິວເຕີ ຂອງ ຍີ່ປຸ່ນ (JPCERT/CC)
- ເຄືອຂ່າຍ OAS/CICTE ຂອງທີມງານຕອບໂຕ້ເຫດການທາງໄຊເບີ (CSIRT) ຂອງລັດຖະບານ ອາເມຣິກາ
- ໜ່ວຍງານຮັກສາຄວາມປອດໄພທາງໄຊເບີ ຂອງ ສິງກະໂປ (CSA)
- ໜ່ວຍງານຄວາມປອດໄພທາງໄຊເບີ ແລະ ຂໍ້ມູນຂ່າວສານແຫ່ງຊາດ ຂອງສາທາລະນະລັດເຊັກ(NÚKIB)

ອົງກອນຜູ້ຂຽນຮັບຮູ້ເຖິງການມີການປະກອບສ່ວນຂອງຄູ່ຮ່ວມງານຂອງພາກເອກະຊົນຈຳນວນຫຼາຍໃນການພັດທະນາດ້ານຄວາມປອດໄພໂດຍການອອກແບບ ແລະ ຄວາມປອດໄພໂດຍຄ່າເລີ່ມຕົ້ນ. ຜະລິດຕະພັນນີ້ແມ່ນມີຈຸດປະສົງເພື່ອສ້າງຄວາມກ້າວໜ້າໃນການສົນທະນາ ລະຫວ່າງປະເທດກ່ຽວກັບລຳດັບຄວາມສຳຄັນ ການລົງທຶນ ແລະ ການຕັດສິນໃຈທີ່ຈຳເປັນເພື່ອໃຫ້ບັນລຸອະນາຄົດທີ່ເທັກໂນໂລຢີມີຄວາມປອດໄພ ຄວາມໝັ້ນຄົງ ແລະ ຄວາມທົນທານໂດຍການອອກແບບ ແລະ ຄ່າເລີ່ມຕົ້ນ. ເພື່ອເຮັດສິ່ງນີ້, ອົງກອນຜູ້ຂຽນຈຶ່ງຊອກຫາຄຳຕິຊົມກ່ຽວກັບຜະລິດຕະພັນນີ້ຈາກພາກສ່ວນ ທີ່ສົນໃຈ ແລະ ຕັ້ງໃຈຈະຈັດກອງປະຊຸມຮັບຟັງຫຼາຍໆຄັ້ງເພື່ອປັບປຸງ ກຳນົດ ແລະ ພັດທະນາ ຄຳແນະນຳຂອງພວກເຮົາເພີ່ມເຕີມເພື່ອໃຫ້ບັນລຸເປົ້າໝາຍຮ່ວມກັນຂອງພວກເຮົາ.

ສຳລັບຂໍ້ມູນເພີ່ມເຕີມກ່ຽວກັບຄວາມສຳຄັນຂອງຄວາມປອດໄພຂອງຜະລິດຕະພັນ, ຈົ່ງເບິ່ງບົດຄວາມຂອງ CISA, ຄ່າໃຊ້ຈ່າຍຂອງເທັກໂນໂລຢີ ທີ່ບໍ່ປອດໄພ ແລະ ສິ່ງທີ່ພວກເຮົາສາມາດເຮັດໄດ້ກ່ຽວກັບເທັກໂນໂລຢີ ດັ່ງກ່າວ.

[2] ຕໍ່ໄປນີ້ຈະເອີ້ນວ່າ ອົງກອນຜູ້ຂຽນ.

ມີຫຍັງໃໝ່

ການພິມເຜີຍແຜ່ເບື້ອງຕົ້ນຂອງບົດລາຍງານນີ້ໄດ້ເຮັດໃຫ້ເກີດການສົນທະນາຢ່າງຫຼວງຫຼາຍໃນອຸດສາຫະກຳຊອບແວ. ຂ່າວປະຈຳວັນ ຂອງອົງກອນ ແລະ ບຸກຄົນທີ່ຖືກບຸກລຸກຊີ້ໃຫ້ເຫັນຄວາມຈຳເປັນໃນການສົນທະນາເພີ່ມເຕີມກ່ຽວກັບວິທີການແກ້ໄຂບັນຫາຊ້ຳເຮື້ອ ແລະ ເປັນລະບົບໃນຜະລິດຕະພັນ ຊອບແວ.

ຫຼັງຈາກການເປີດຕົວໃນເດືອນເມສາ 2023, ອົງກອນຜູ້ຂຽນ (ຕໍ່ຈາກນີ້ ໄປເອີ້ນວ່າ "ພວກເຮົາ" ແລະ "ຂອງພວກເຮົາ") ໄດ້ຮັບຄຳ ຄິດຄຳຄິດເຫັນ ຈາກ ບຸກຄົນ, ບໍລິສັດ ແລະ ສະມາຄົມການຄ້າຫຼາຍຮ້ອຍລາຍ. ຄຳຮ້ອງຂໍທີ່ພົບພໍ້ເລື້ອຍທີ່ສຸດໃນຄຳຕິຊົມແມ່ນການ ໃຫ້ລາຍລະອຽດເພີ່ມເຕີມກ່ຽວກັບສາມຫຼັກການທີ່ໃຊ້ກັບທັງຜູ້ຜະລິດຊອບແວ ແລະ ລູກຄ້າຂອງພວກເຂົາ. ໃນເອກະສານນີ້ ພວກ ເຮົາຈະຂະຫຍາຍບົດລາຍງານຕົ້ນສະບັບ ແລະ ກ່າວເຖິງຫົວຂໍ້ອື່ນໆ ເຊັ່ນ ຜູ້ຜະລິດ ແລະ ຂະໜາດລູກຄ້າ, ການເຕີບໂຕເຕັມທີ່ຂອງ ລູກຄ້າ ແລະ ຂອບເຂດ ຂອງຫຼັກການ.

ຊອບແວແມ່ນມີຢູ່ທົ່ວທຸກແຫ່ງ ແລະ ບໍ່ມີບົດລາຍງານໃດທີ່ຈະສາມາດຄວບຄຸມ ລະບົບຊອບແວທັງໝົດ ການພັດທະນາຜະລິດຕະ ພັນຊອບແວ ແລະ ການປະຕິບັດ ແລະ ການບຳລຸງ ຮັກສາຂອງລູກຄ້າ ແລະ ການເຊື່ອມໂຍງກັບລະບົບອື່ນໆໄດ້ຢ່າງພຽງພໍ. ສຳລັບ ຄຳແນະນຳຂ້າງລຸ່ມນີ້ທີ່ບໍ່ໄດ້ກຳນົດຢ່າງຊັດເຈນກັບສະພາບແວດລ້ອມສະເພາະໃດໜຶ່ງ ພວກເຮົາຫວັງວ່າຈະໄດ້ຍິນຈາກຊຸມຊົນວ່າ ແນວທາງປະຕິບັດທີ່ໄດ້ອະທິບາຍ ໄວ້ໃນເອກະສານນີ້ນຳໄປສູ່ການປັບປຸງ ຄວາມປອດໄພໂດຍສະເພາະຢ່າງໃດ.

ບົດລາຍງານນີ້ໃຊ້ກັບຜູ້ຜະລິດລະບົບຊອບແວປັນຍາປະດິດ (AI) ແລະ ແບບຈຳລອງ ເຊັ່ນກັນ. ເຖິງແມ່ນວ່າອາດຈະແຕກຕ່າງຈາກ ຮູບແບບຂອງຊອບແວແບບດັ້ງເດີມແຕ່ຫຼັກ ການປະຕິບັດດ້ານຄວາມປອດໄພຂັ້ນພື້ນຖານຍັງຄົງໃຊ້ກັບລະບົບ ແລະ ແບບຈຳລອງ AI ແນວປະຕິບັດດ້ານຄວາມປອດໄພດ້ວຍການອອກແບບບາງຢ່າງ ອາດຈະ ຕ້ອງມີການດັດ ແກ້ເພື່ອຮັບຮູ້ການພິຈາລະນາສະເພາະ ຂອງ AI, ແຕ່ຫຼັກການທັງສາມຢ່າງດ້ານປອດໄພ ໂດຍຫຼັກການການອອກແບບນັ້ນນຳໄປໃຊ້ກັບທຸກລະບົບ ຂອງ AI.

ພວກເຮົາຮັບຮູ້ວ່າການປ່ຽນແປງວົງຈອນການພັດທະນາຊອບແວ (SDLC) ເພື່ອໃຫ້ສອດຄ່ອງກັບຫຼັກການອອກແບບທີ່ປອດໄພ ເຫຼົ່ານີ້ບໍ່ແມ່ນວຽກງານທີ່ງ່າຍດາຍ ແລະ ອາດຈະຕ້ອງໃຊ້ເວລາ. ນອກຈາກນັ້ນ, ຜູ້ຜະລິດຊອບແວລາຍນ້ອຍອາດຈະປະສົບບັນຫາໃນ ການນຳປະຕິບັດ ຄຳແນະນຳເຫຼົ່ານີ້. ພວກເຮົາເຊື່ອວ່າອຸດສາຫະກຳຊອບແວຈຳເປັນຕ້ອງມີເຄື່ອງມື ແລະ ຂັ້ນຕອນຕ່າງໆທີ່ສາມາດໃຊ້ ໄດ້ຢ່າງກວ້າງຂວາງທີ່ເຮັດໃຫ້ຜະລິດຕ ພັນປອດໄພ ຍິ່ງຂຶ້ນ. ເນື່ອງຈາກຜູ້ຄົນ ແລະ ອົງກອນຕ່າງໆສຸມຄວາມສົນໃຈໄປໃສ່ການປັບປຸງ ຄວາມປອດໄພຂອງຊອບແວຫຼາຍຂຶ້ນ ພວກເຮົາເຊື່ອວ່າມີບ່ອນຫວ່າງສຳລັບການປະດິດສ້າງທີ່ຈະຮັດແຄບ ຊ່ອງຫວ່າງລະຫວ່າງຜູ້ ຜະລິດຊອບແວລາຍໃຫຍ່ ແລະ ລາຍນ້ອຍລົງເພື່ອຜົນປະໂຫຍດ ຂອງລູກຄ້າທັງໝົດ.

ການອັບເດດບົດລາຍງານການອອກແບບໂດຍປອດໄພສະບັບຕົ້ນນີ້ເປັນສ່ວນໜຶ່ງຂອງຄວາມມຸ່ງໝັ້ນ ຂອງພວກເຮົາໃນການສ້າງ ຄວາມຮ່ວມມືກັບຊຸມຊົນທີ່ມີສ່ວນກ່ຽວຂ້ອງຈຳນວນ ຫຼາຍທີ່ເປັນຮາກຖານຂອງລະບົບນິເວດ ທາງເທັກໂນໂລຢີຂອງພວກເຮົາ. ມັນ ແມ່ນຜົນມາຈາກຄຳຄິດຄຳເຫັນຈາກຫຼາຍພາກສ່ວນຂອງລະບົບນິເວດນັ້ນ ແລະ ພວກ ເຮົາຈະຮັບຟັງ ແລະ ຮຽນຮູ້ຈາກທັດສະນະມຸມ ມອງຕໍ່ໄປ. ເຖິງວ່າຈະມີສິ່ງທ້າທາຍຫຼາຍຢ່າງລໍຖ້າຢູ່ຂ້າງໜ້າກໍຕາມ ພວກເຮົາມີຄວາມຫວັງໃນແງ່ດີ ຢ່າງບໍ່ໜ້າເຊື່ອຍ້ອນວ່າພວກເຮົາ ຮຽນຮູ້ເພີ່ມເຕີມກ່ຽວກັບ ຜູ້ຄົນ ແລະ ອົງກອນທີ່ໄດ້ຮັບຮອງເອົາປັດຊະຍາ ຄວາມປອດໄພໂດຍການ ອອກແບບມາໃຊ້ແລ້ວ ຊຶ່ງມັກ ຈະປະສົບຜົນສຳເລັດ.

ວິທີນຳໃຊ້ເອກະສານນີ້

ພວກເຮົາຂໍຮຽກຮ້ອງໃຫ້ຜູ້ຜະລິດຊອັບແວປະຕິບັດຕາມຫຼັກການໃນເອກະສານນີ້. ຜູ້ຜະລິດຊອັບແວສາມາດສະແດງໃຫ້ເຫັນເຖິງຄວາມມຸ່ງໝັ້ນຂອງພວກເຂົາໂດຍການບັນ ທຶກການດຳເນີນການຂອງພວກເຂົາຕໍ່ສາທາລະນະໃຫ້ສອດຄ່ອງກັບຂັ້ນຕອນຂ້າງລຸ່ມນີ້. ພວກເຮົາຊຸກຍູ້ໃຫ້ຜູ້ຜະລິດຊອັບແວຊອກຫາຍຸດທະວິທີທີ່ສອດຄ່ອງກັບເຈດຕະນາຂອງຫຼັກການນີ້ ແລະ ສ້າງສິ່ງປະດິດທີ່ຈະສ້າງກໍລະນີທີ່ໜ້າສົນໃຈກັບລູກຄ້າໃນປະຈຸບັນ ແລະ ຜູ້ທີ່ມີໂອກາດເປັນລູກຄ້າບໍ່ຄ່ອຍເຊື່ອງ່າຍໆວ່າພວກເຂົາກຳລັງ ລວບລວມ ຄວາມປອດໄພ ດ້ວຍ ປັດຊະຍາການອອກແບບ.

ນອກເໜືອຈາກການດຳເນີນການທີ່ຜູ້ຜະລິດຊອັບແວຄວນປະຕິບັດແລ້ວ ລູກຄ້າຍັງສາມາດໃຊ້ປະໂຫຍດຈາກເອກະສານນີ້ໄດ້ອີກດ້ວຍ. ບໍລິສັດທີ່ຊື້ຊອັບແວຄວນຖາມຄຳຖາມທີ່ຍາກໆກັບຜູ້ຈຳໜ່າຍໂດຍໄດ້ຮັບແຮງບັນດານໃຈ ຈາກຕົວຢ່າງຂອງ ການປະຕິບັດຕາມຫຼັກການທີ່ລະບຸໄວ້ໃນເອກະສານນີ້. ການເຮັດດັ່ງນີ້ ລູກຄ້າສາມາດຊ່ວຍປ່ຽນຕະຫຼາດໄປສູ່ຜະລິດຕະພັນທີ່ມີຄວາມປອດໄພຫຼາຍຂຶ້ນໂດຍການອອກແບບ. ຕົວຢ່າງຂອງຄຳຖາມທີ່ລູກຄ້າສາມາດຖາມຜູ້ຂາຍແມ່ນມີໃຫ້ຢູ່ໃນ ຄຳແນະນຳຂອງ CISA ສຳລັບການຊື້ເທັກໂນໂລຢີ K-12.

ພວກເຮົາຊຸກຍູ້ໃຫ້ລູກຄ້າວິສາຫະກິດລວມເອົາການປະຕິບັດເຫຼົ່ານີ້ເຂົ້າໃນຂະບວນການຈັດຊື້ ຈັດຈ້າງ ການປະເມີນການກວດສອບສະຖານະຂອງຜູ້ຂາຍ ການຕັດສິນໃຈ ຍອມຮັບ ຄວາມສ່ຽງຂອງວິສາຫະກິດ ແລະ ຂັ້ນຕອນອື່ນໆທີ່ດຳເນີນການໃນ ເວລາປະເມີນຜູ້ຂາຍ. ລູກຄ້າຄວນຊຸກດັນໃຫ້ຜູ້ຂາຍຂອງພວກເຂົາເຮັດເອກະສານກ່ຽວກັບຄວາມປອດໄພຕໍ່ສະທາລະນະ ໂດຍການປະຕິບັດການອອກແບບທີ່ຜູ້ຂາຍແຕ່ລະຄົນເຮັດ. ໂດຍລວມແລ້ວ, ສິ່ງນີ້ສາມາດສ້າງສັນຍານຄວາມຕ້ອງການທີ່ ເຂັ້ມແຂງດ້ານຄວາມປອດໄພ ເຊິ່ງສາມາດສົ່ງເສີມ ແລະ ເຮັດໃຫ້ຜູ້ຜະລິດຊອັບແວສາມາດກ້າວໄປສູ່ຂັ້ນຕອນການຮັກສາ ຄວາມປອດໄພທີ່ຫຼາຍຂຶ້ນ. ເວົ້າອີກແນວໜຶ່ງ, ເຊັ່ນດຽວກັນກັບທີ່ພວກເຮົາຊອກຫາການສ້າງຄວາມປອດໄພ ທີ່ແຜ່ຂະຫຍາຍໂດຍປັດຊະຍາການອອກແບບພາຍໃນຜູ້ຜະລິດຊອັບແວ ພວກເຮົາຈຳເປັນຕ້ອງສ້າງວັດທະນະທຳ "ປອດໄພໂດຍຄວາມຕ້ອງການ" ກັບລູກຄ້າຂອງພວກເຂົາ.

ความปลอดภัยโดยการออกแบบ

"ການຮັກສາຄວາມປອດໄພໂດຍການອອກແບບ" ໝາຍຄວາມວ່າຜະລິດຕະພັນເທັກໂນໂລຢີ ຖືກສ້າງຂຶ້ນໃນແບບທີ່ສົມເຫດສົມຜົນເພື່ອປົກປ້ອງຜູ້ກະທຳຄວາມຜິດ ທາງໄຊເບີ ທີ່ປະສົງຮ້າຍໃນການເຂົ້າເຖິງອຸປະກອນ ຂໍ້ມູນ ແລະ ໂຄງສ້າງ ພື້ນຖານທີ່ເຊື່ອມຕໍ່ໄດ້ສຳເລັດ. ຜູ້ຜະລິດຊອັບແວຄວນທຳການປະເມີນຄວາມສ່ຽງເພື່ອກຳນົດ ແລະ ລະບຸ ໄພຂົ່ມຂູ່ທາງໄຊເບີທີ່ແຜ່ຫຼາຍຕໍ່ລະບົບທີ່ສຳຄັນ ແລະ ຫຼັງຈາກນັ້ນລວມການປົກປ້ອງໄວ້ໃນແບບແຜນຜະລິດຕະພັນທີ່ຄຳນຶງເຖິງ ໄພຂົ່ມຂູ່ທາງໄຊເບີທີ່ກຳລັງພັດທະນາ.

ແນວທາງປະຕິບັດໃນການພັດທະນາເທັກໂນໂລຢີຂໍ້ມູນຂ່າວສານ(IT) ທີ່ປອດໄພ ແລະ ການປ້ອງກັນຫຼາຍຊັ້ນ ທີ່ເອີ້ນວ່າ ການປ້ອງກັນໃນທາງເລິກຍັງໄດ້ຮັບການແນະນຳເພື່ອປ້ອງ ກັນ ຜູ້ປະສົງບໍ່ດີຈາກການໂຈມຕີລະບົບ ຫຼື ການເຂົ້າເຖິງຂໍ້ມູນ ທີ່ລະອຽດອ່ອນໂດຍ ບໍ່ໄດ້ ຮັບອະນຸຍາດ. ອົງກອນຜູ້ຂຽນຍັງແນະນຳຕື່ມອີກວ່າໃຫ້ຜູ້ຜະລິດໃຊ້ຮູບແບບໄພຂົ່ມຂູ່ທີ່ ໄດ້ຮັບການປັບ ແຕ່ງໃນລະຫວ່າງຂັ້ນຕອນການພັດທະນາຜະລິດຕະພັນເພື່ອແກ້ໄຂໄພຂົ່ມຂູ່ທີ່ອາດເກີດຂຶ້ນກັບລະບົບ ແລະ ບັນຊີສຳລັບຂະບວນການນຳໃຊ້ຂອງແຕ່ລະລະບົບ.

ອົງກອນຜູ້ຂຽນຮຽກຮ້ອງໃຫ້ຜູ້ຜະລິດໃຊ້ວິທີການຮັກສາຄວາມປອດໄພແບບລວມສຳລັບ ຜະລິດຕະພັນ ແລະ ເວທີຂອງຕົນ ຄວາມປອດໄພໂດຍການພັດທະນາການອອກແບບຈຳເປັນຕ້ອງມີການລົງທຶນໃນທາງຍຸດທະສາດໃນ ຊັບພະຍາກອນສະເພາະໂດຍຜູ້ຜະລິດຊອັບແວໃນແຕ່ລະຊັ້ນຂອງຂະບວນການ ອອກແບບ ແລະ ການພັດທະນາ ຜະລິດຕະພັນທີ່ບໍ່ສາມາດ "ຍຶດຕິດ"ໄດ້ໃນພາຍຫຼັງ. ມັນຈຳເປັນຕ້ອງມີຄວາມເປັນຜູ້ນຳທີ່ເຂັ້ມແຂງຈາກຜູ້ບໍລິຫານ ທຸລະກິດຊັ້ນນຳຂອງຜູ້ຜະລິດເພື່ອເຮັດໃຫ້ຄວາມປອດໄພມີຄວາມສຳຄັນທາງທຸລະກິດ ບໍ່ແມ່ນພຽງແຕ່ເປັນຄຸນສົມບັດ ທາງເທັກນິກເທົ່ານັ້ນ. ການຮ່ວມມືລະຫວ່າງຜູ້ນຳທຸລະກິດ ແລະ ທີມງານດ້ານເທັກນິກນີ້ຂະຫຍາຍອອກຈາກຕັ້ງແຕ່ ຂັ້ນຕອນເບື້ອງຕົ້ນຂອງການອອກແບບ ແລະ ການພັດທະນາ ໂດຍຜ່ານການນຳໃຊ້ ແລະ ການບຳລຸງຮັກສາຂອງລູກຄ້າ. ຜູ້ຜະລິດໄດ້ຮັບການຊຸກຍູ້ໃຫ້ມີການແລກປ່ຽນ ແລະ ການລົງທຶນຢ່າງໜັກ ລວມທັງສິ່ງທີ່ຈະ "ເບິ່ງບໍ່ເຫັນ" ໃຫ້ກັບລູກຄ້າ (ເຊັ່ນ: ການເຄື່ອນຍ້າຍໄປສູ່ພາສາການຂຽນໂປຣແກຣມທີ່ຊ່ວຍກຳຈັດຊ່ອງໂຫວ່ທີ່ແພ່ຫຼາຍ). ພວກເຂົາຄວນຈັດລຳດັບ ຄວາມສຳຄັນຂອງຄຸນສົມບັດ ກົນໄກ ແລະ ການໃຊ້ເຄື່ອງມືທີ່ປົກປ້ອງລູກຄ້າຫຼາຍກວ່າແທນທີ່ຈະເປັນຄຸນສົມບັດຂອງ ຜະລິດຕະພັນທີ່ເບິ່ງຄືວ່າໜ້າສົນໃຈແຕ່ຂະຫຍາຍຂອບເຂດການໂຈມຕີ.

ບໍ່ມີວິທີແກ້ບັນຫາດຽວທີ່ຈະຢຸດໄພຂົ່ມຂູ່ທີ່ເກີດຂຶ້ນຢ່າງຕໍ່ເນື່ອງຂອງຜູ້ປະສົງຮ້າຍ ທາງໄຊເບີ ທີ່ເປັນອັນຕະລາຍທີ່ສວຍ ໃຊ້ຊ່ອງໂຫວ່ດ້ານເທັກໂນໂລຢີ ແລະ ຜະລິດຕະພັນທີ່ "ປອດໄພໂດຍການອອກແບບ" ຈະຍັງຄົງປະສົບກັບຄວາມສ່ຽງ ຕໍ່ໄປ; ແນວໃດກໍ່ຕາມ, ຊ່ອງໂຫວ່ຊຸດໃຫຍ່ແມ່ນເນື່ອງມາຈາກ ສາເຫດຫຼັກທີ່ຂ້ອນຂ້າງນ້ອຍ. ຜູ້ຜະລິດຄວນສ້າງ ແຜນງານທີ່ເປັນລາຍລັກອັກສອນເພື່ອຈັດວາງກຸ່ມຜະລິດຕະພັນທີ່ມີຢູ່ຂອງພວກເຂົາໃຫ້ມີຄວາມປອດໄພຫຼາຍຂຶ້ນໂດຍ ຫຼັກການປະຕິບັດການອອກແບບເພື່ອໃຫ້ແນ່ໃຈວ່າຈະບ່ຽງເບນໃນສະຖານະການພິເສດເທົ່ານັ້ນ.

ອົງກອນຜູ້ຂຽນຮັບຮູ້ວ່າການເປັນເຈົ້າຂອງຜົນໄດ້ຮັບດ້ານຄວາມປອດໄພສຳລັບລູກຄ້າ ແລະ ການຮັບປະກັນ ຄວາມປອດໄພຂອງລູກຄ້າໃນລະດັບນີ້ອາດຈະເພີ່ມຄ່າໃຊ້ຈ່າຍໃນການພັດທະນາ. ຢ່າງໃດກໍຕາມ, ການລົງທຶນໃນດ້ານ ຄວາມປອດໄພໂດຍແນວທາງການ ອອກແບບໄປພ້ອມກັບການພັດທະນາຜະລິດຕະພັນເທັກໂນໂລຢີທີ່ເປັນມະວັດຕະ ກຳ ແລະ ການບຳລຸງຮັກສາທີ່ມີຢູ່ແລ້ວສາມາດປັບປຸງທ່າທາງຄວາມປອດໄພຂອງລູກຄ້າໄດ້ຢ່າງຫຼວງຫຼາຍ ແລະ ຫຼຸດຜ່ອນ ຄວາມເປັນໄປໄດ້ຂອງ ການປະນີປະນອມ. ການຮັກສາຄວາມປອດໄພໂດຍຫຼັກການການອອກແບບບໍ່ພຽງແຕ່ເສີມສ້າງ ຄວາມເຂັມແຂງໃຫ້ແກ່ມາດຕາການຮັກສາຄວາມປອດໄພສຳລັບລູກຄ້າ ແລະ ຊື່ສຽງຂອງຍີ່ຫໍ້ສຳລັບນັກພັດທະນາ ເທົ່ານັ້ນ ແຕ່ການປະຕິບັດນີ້ຍັງຊ່ວຍຫຼຸດຄ່າໃຊ້ຈ່າຍໃນການບຳລຸງຮັກສາ ແລະ ການແພັດຊິງ (patching) ສຳລັບ ຜູ້ຜະລິດໃນໄລຍະຍາວອີກດ້ວຍ.

ຄຳແນະນຳສຳລັບຜູ້ຜະລິດຊອັບແວທີ່ລະບຸໄວ້ຂ້າງລຸ່ມນີ້ສະແດງບັນຊີລາຍການຂອງແນວທາງປະຕິບັດ ແລະ ນະໂຍບາຍ ການພັດທະນາຜະລິດຕະພັນ ສຳລັບຜູ້ຜະລິດທີ່ຈະຕ້ອງພິຈາລະນາ.

ຄວາມປອດໄພໂດຍຄ່າເລີ່ມຕົ້ນ

"ຄວາມປອດໄພໂດຍຄ່າເລີ່ມຕົ້ນ" ໝາຍຄວາມວ່າຜະລິດຕະພັນມີຄວາມທົນທານຕໍ່ກັບເທັກນິກການສະແຫວງຫາຜົນປະໂຫຍດທີ່ແຜ່ຫຼາຍໄດ້ທັນທີໂດຍບໍ່ມີຄ່າໃຊ້ຈ່າຍເພີ່ມເຕີມ. ຜະລິດຕະພັນເຫຼົ່ານີ້ປ້ອງກັນໄພຂົ່ມຂູ່ ແລະ ຄວາມສ່ຽງທີ່ແຜ່ຫຼາຍໂດຍທີ່ຜູ້ໃຊ້ ບໍ່ຕ້ອງໃຊ້ ຂັ້ນຕອນເພີ່ມເຕີມເພື່ອຮັກສາຄວາມປອດໄພໃຫ້ພວກເຂົາ. ຜະລິດຕະພັນທີ່ປອດໄພໂດຍຄ່າເລີ່ມຕົ້ນຖືກອອກແບບມາເພື່ອເຮັດໃຫ້ລູກຄ້າຮັບຮູ້ຢ່າງຊັດແຈ້ງວ່າເມື່ອພວກເຂົາຫັນເຫໄປຈາກຄ່າເລີ່ມຕົ້ນທີ່ປອດໄພ, ພວກເຂົາກຳລັງເພີ່ມຄວາມ ເປັນໄປໄດ້ຂອງການປະນີປະນອມຫຼາຍຂຶ້ນເວັ້ນເສັຍແຕ່ວ່າພວກເຂົາຈະໃຊ້ການຄວບຄຸມ ການຊົດເຊີຍເພີ່ມເຕີມ. ຄວາມປອດໄພໂດຍຄ່າເລີ່ມຕົ້ນແມ່ນຮູບແບບຂອງຄວາມປອດໄພໂດຍການອອກແບບ.

- ການກຳນົດ ຄ່າທີ່ປອດໄພຄວນຈະເປັນພື້ນຖານເລີ່ມຕົ້ນ. ຜະລິດຕະພັນປອດໄພໂດຍຄ່າເລີ່ມຕົ້ນເຮັດໃຫ້ການຄວບຄຸມຄວາມປອດໄພທີ່ສຳຄັນທີ່ສຸດທີ່ຈຳເປັນເພື່ອປົກປ້ອງອົງກອນ ຈາກຜູ້ກະທຳຄວາມຜິດທາງໄຊເບີໂດຍອັດຕະໂນມັດ ລວມທັງໃຫ້ຄວາມສາມາດໃນການນຳໃຊ້ ແລະ ກຳນົດຄ່າການຄວບຄຸມຄວາມປອດໄພເພີ່ມເຕີມໂດຍບໍ່ມີຄ່າໃຊ້ຈ່າຍເພີ່ມເຕີມ.

- ຄວາມຊັບຊ້ອນຂອງການຕັ້ງຄ່າຄວາມປອດໄພບໍ່ຄວນເປັນບັນຫາຂອງລູກຄ້າ. ພະນັກງານໄອທີຂອງອົງກອນແມ່ນມີໜ້າທີ່ຮັບຜິດຊອບດ້ານຄວາມປອດໄພ ແລະ ການປະ ຕິບັດການຫຼາຍເກີນໄປ, ດັ່ງນັ້ນຈຶ່ງສົ່ງຜົນໃຫ້ມີເວລາຈຳກັດເພື່ອທຳການເຂົ້າໃຈ ແລະ ປັບໃຊ້ຜົນກະທົບດ້ານຄວາມປອດໄພ ແລະ ການຫຼຸດຜ່ອນທີ່ຈຳເປັນສຳລັບ ທ່າທາງ ຄວາມ ປອດໄພທາງໄຊເບີທີ່ເຂັ້ມແຂງ. ຜູ້ຜະລິດສາມາດຊ່ວຍເຫຼືອລູກຄ້າຂອງພວກເຂົາໄດ້ໂດຍການເພີ່ມປະສິດທິພາບການກຳນົດຄ່າຜະລິດຕະພັນທີ່ປອດໄພ - ຮັບປະກັນ "ເສັ້ນທາງເລີ່ມຕົ້ນ" - ຮັບປະກັນວ່າຜະລິດ ຕະພັນ ຂອງພວກເຂົາຖືກຜະລິດ, ແຈກຢາຍ ແລະ ນຳໃຊ້ຢ່າງປອດໄພຕາມມາດຕະຖານ "ຄວາມປອດໄພໂດຍຄ່າເລີ່ມຕົ້ນ".

ຜູ້ຜະລິດຜະລິດຕະພັນທີ່ "ປອດໄພໂດຍຄ່າເລີ່ມຕົ້ນ" ບໍ່ໄດ້ຄິດຄ່າເພີ່ມເຕີມສຳລັບການໃຊ້ ການຕັ້ງຄ່າຄວາມປອດໄພເພີ່ມເຕີມ. ແທນທີ່ຈະຄິດຄ່າເພີ້ມ, ແຕ່ຈະລວມເອົາໄວ້ໃນຜະລິດຕະພັນພື້ນຖານແທນ ເຊັ່ນ ສາຍແອວ ນິລະໄພຈະລວມຢູ່ໃນລົດໃໝ່ທຸກໆຄັນ.

ຄວາມປອດໄພບໍ່ຄວນເປັນທາງເລືອກທີ່ຟຸ່ມເຟືອຍ, ແຕ່ຄວນຖືວ່າເປັນສິດທີ່ລູກຄ້າຈະໄດ້ຮັບໂດຍບໍ່ມີການເຈລະຈາ ຫຼື ຈ່າຍເງິນເພີ່ມເຕີມ.

ຄຳແນະນຳສຳລັບຜູ້ຜະລິດຊອັບແວ

ຄູ່ມືຮ່ວມນີ້ໃຫ້ຄຳແນະນຳແກ່ຜູ້ຜະລິດສຳລັບການພັດທະນາແຜນງານທີ່ເປັນລາຍລັກອັກສອນ ເພື່ອນຳໄປປະຕິບັດ ແລະ ຮັບປະກັນຄວາມປອດໄພດ້ານໄອທີ. ອົງກອນຜູ້ຂຽນແນະນຳໃຫ້ຜູ້ຜະລິດຊອັບແວໃຊ້ຍຸດທະວິທີທີ່ລະບຸໄວ້ໃນພາກສ່ວນຂ້າງລຸ່ມນີ້ເພື່ອເປັນເຈົ້າຂອງຜົນໄດ້ຮັບດ້ານຄວາມປອດໄພຂອງລູກຄ້າຂອງພວກເຂົາໂດຍຜ່ານຄວາມປອດໄພໂດຍການອອກແບບ ແລະ ຫຼັກການເລີ່ມຕົ້ນ.

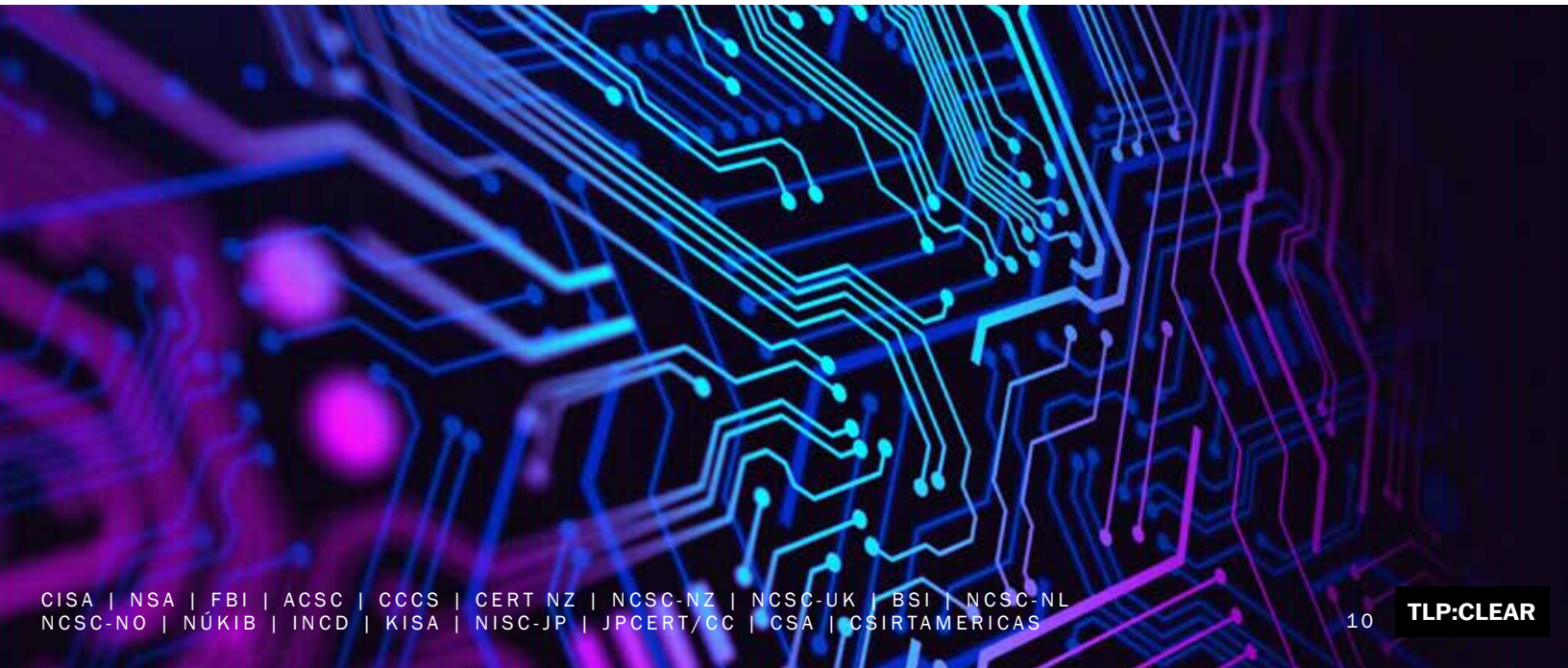
ຫຼັກການຮັກສາຄວາມປອດໄພຂອງຜະລິດຕະພັນຊອັບແວ

ຜູ້ຜະລິດຊອັບແວໄດ້ຮັບການຊຸກຍູ້ໃຫ້ປັບໃຊ້ຈຸດສຸມຍຸດທະສາດທີ່ໃຫ້ຄວາມສຳຄັນກັບ ຄວາມປອດໄພຂອງຊອັບແວ. ອົງກອນຜູ້ຂຽນໄດ້ພັດທະນາສາມຫຼັກການຕໍ່ໄປນີ້ເພື່ອເປັນແນວທາງແກ່ຜູ້ຜະລິດຊອັບແວໃນການສ້າງຄວາມປອດໄພຂອງ ຊ ອັບແວເຂົ້າໃນຂະບວນການອອກແບບຂອງພວກເຂົາ ກ່ອນທີ່ຈະພັດທະນາ ການຕັ້ງຄ່າ ແລະ ການຂົນສົ່ງຜະລິດຕະພັນຂອງຕົນ

1 **ເປັນເຈົ້າຂອງຜົນໄດ້ຮັບດ້ານຄວາມປອດໄພຂອງລູກຄ້າ** ແລະ ພັດທະນາຜະລິດຕະພັນຕາມຄວາມເໝາະສົມ. ພາລະດ້ານ ຄວາມປອດໄພບໍ່ຄວນຕົກຢູ່ກັບລູກຄ້າພຽງຜູ້ດຽວ.

2 **ຮັບເອົາຄວາມໂປ່ງໃສ ແລະ ຄວາມຮັບຜິດຊອບທີ່ຮຸນແຮງ.**
ຜູ້ຜະລິດຊອັບແວຄວນມີຄວາມພາກພູມໃຈໃນການສະໜອງຜະລິດຕະພັນທີ່ປອດໄພ ແລະ ໝັ້ນຄົງ ເຊັ່ນດຽວກັນກັບ ການແຍກຕົວເອງຈາກສ່ວນທີ່ເຫຼືອຂອງຊຸມຊົນຜູ້ຜະລິດອື່ນໆ ໂດຍອີງໃສ່ຄວາມສາມາດໃນການເຮັດຂອງຕົນເອງ. ນີ້ອາດຈະລວມເຖິງການແບ່ງປັນຂໍ້ມູນທີ່ພວກເຂົາຮຽນຮູ້ຈາກການປັບໃຊ້ຂອງລູກຄ້າຂອງ ພວກເຂົາ, ເຊັ່ນການໃຊ້ກົນໄກ ການກວດສອບທີ່ເຂັ້ມແຂງຮັດກຸມໂດຍຄ່າເລີ່ມຕົ້ນ. ນອກຈາກນີ້ ຍັງລວມເຖິງຄວາມມຸ່ງໝັ້ນທີ່ແຮງກ້າເພື່ອໃຫ້ແນ່ໃຈວ່າ ຄຳແນະນຳ ກ່ຽວ ກັບຈຸດອ່ອນ ແລະ ການບັນທຶກຄວາມສ່ຽງທົ່ວໄປ ແລະ ການເປີດເຜີຍຂໍ້ມູນ (CVE) ທີ່ກ່ຽວຂ້ອງນັ້ນ ແມ່ນຄົບຖ້ວນ ແລະ ຖືກຕ້ອງ. ຢ່າງໃດກໍ່ຕາມ, ຈົ່ງລະວັງການລໍ້ລວງທີ່ຈະນັບ CVEs ເປັນຕົວຊີ້ທາງລົບ ເນື່ອງຈາກວ່າ ຕົວເລກດັ່ງກ່າວຍັງເປັນສັນຍານຂອງຊຸມຊົນທີ່ມີການວິເຄາະ ແລະ ການທົດສອບລະຫັດທີ່ດີອີກດ້ວຍ.

3 **ສ້າງໂຄງປະກອບການຈັດຕັ້ງ ແລະ ຄວາມເປັນຜູ້ນຳເພື່ອບັນລຸ ເປົ້າໝາຍ ເຫຼົ່ານີ້.**
ເຖິງແມ່ນວ່າຄວາມຊ່ຽວຊານດ້ານວິຊາສະເພາະແມ່ນມີຄວາມສຳຄັນຕໍ່ຄວາມປອດໄພຂອງ ຜະລິດຕະພັນກໍຕາມ ຜູ້ບໍລິຫານລະດັບສູງແມ່ນຜູ້ມີອຳນາດຕັດສິນໃຈຫຼັກສຳລັບການປະຕິ ບັດການປ່ຽນແປງໃນອົງກອນ. ຜູ້ບໍລິຫານຈຳເປັນຕ້ອງຈັດລຳດັບຄວາມສຳຄັນຂອງຄວາມປອດໄພເປັນອົງປະກອບສຳຄັນຂອງການພັດທະນາ ຜະລິດຕະພັນໃນທົ່ວອົງກອນ ແລະ ການຮ່ວມມືກັບລູກຄ້າ.



ເພື່ອໃຫ້ເປັນໄປຕາມສາມຫຼັກການນີ້ ຜູ້ຜະລິດຄວນພິຈາລະນາວິທີການປະຕິບັດງານ ຫຼາຍ ຢ່າງເພື່ອພັດທະນາຂະບວນການພັດທະນາຂອງ ພວກເຂົາ.

ຈັດກອງປະຊຸມປົກກະຕິກັບຜູ້ບໍລິຫານຂອງບໍລິສັດເພື່ອຊຸກຍູ້ຄວາມສຳຄັນຂອງການຮັກສາຄວາມປອດໄພໂດຍການອອກແບບ ແລະ ຄວາມປອດໄພໂດຍຄ່າເລີ່ມຕົ້ນພາຍໃນອົງກອນ. ນະໂຍບາຍ ແລະ ຂັ້ນຕອນຄວນຈະໄດ້ຮັບການສ້າງຕັ້ງຂຶ້ນເພື່ອມອບລາງວັນໃຫ້ທີມງານ ຜະລິດທີ່ພັດທະນາຜະລິດຕະພັນທີ່ປະຕິບັດຕາມຫຼັກການເຫຼົ່ານີ້ ເຊິ່ງອາດປະກອບມີລາງວັນ ສຳລັບການປະຕິບັດດ້ານຄວາມປອດໄພຂອງຊ ອັບແວທີ່ໂດດເດັ່ນ ຫຼື ແຮງຈູງໃຈສຳລັບຂັ້ນ ໄດວຽກ ແລະ ເງື່ອນໄຂການເລື່ອນຕຳແໜ່ງ.

ດຳເນີນການກ່ຽວກບຄວາມສຳຄັນຂອງຄວາມປອດໄພຂອງຊອັບແວເພື່ອຄວາມສຳເລັດຂອງທຸລະກິດ. ຕົວຢ່າງ, ພິຈາລະນາແຕ່ງຕັ້ງ "ຜູ້ນຳ ດ້ານຄວາມປອດໄພຂອງຊອັບແວ" ຫຼື "ທີມງານ ຄວາມປອດໄພຂອງຊອັບແວ" ທີ່ສະໜັບສະໜູນແນວປະຕິບັດທາງທຸລະກິດ ແລະ ໄອທີ ທີ່ ເຊື່ອມຕໍ່ໂດຍກົງກັບມາດຕະຖານຄວາມປອດໄພຂອງຊອັບແວ ແລະ ຄວາມຮັບຜິດຊອບຂອງຜູ້ຜະລິດ. ຜູ້ຜະລິດຄວນກວດສອບແນ່ໃຈວ່າ ພວກເຂົາມີໂປຣແກຣມການປະເມີນຄວາມປອດໄພຂອງຜະລິດຕະພັນທີ່ເຂັ້ມແຂງ ແລະ ເປັນເອກະລາດສຳລັບຜະລິດຕະພັນຂອງຕົນ.

ໃຊ້ແບບໄພຂົ່ມຂູ່ທີ່ໄດ້ຖືກປັບແຕ່ງມາໃນລະຫວ່າງການຈັດສັນ ແລະ ການພັດທະນາ ຊັບພະຍາກອນ ເພື່ອຈັດລຳດັບຄວາມສຳຄັນຂອງ ລັກສະນະທີ່ມີ ຜົນກະທົບສູງທີ່ສຸດ. ແບບຈຳລອງໄພຂົ່ມຂູ່ຈະພິຈາລະນາກໍລະນີການນຳໃຊ້ສະເພາະຂອງຜະລິດຕະພັນ ແລະ ຊ່ວຍໃຫ້ທີມງານ ພັດທະນາສ້າງຄວາມເຂັ້ມແຂງຜະລິດຕະພັນໄດ້. ສຸດທ້າຍນີ້, ຜູ້ນຳລະດັບສູງຄວນໃຫ້ທີມງານຮັບຜິດຊອບສຳລັບການສົ່ງມອບ ຜະລິດຕະພັນ ທີ່ປອດໄພ ເຊິ່ງເປັນອົງປະກອບທີ່ສຳຄັນທີ່ດີເລີດ ແລະ ຄຸນນະພາບຂອງຜະລິດຕະພັນ.

ໃນສ່ວນໜຶ່ງຂອງການປັບປຸງແນວທາງປະຕິບັດນີ້ໃນເດືອນຕຸລາ 2023 ສາມຫຼັກການເຫຼົ່ານີ້ແມ່ນໄດ້ຮັບການຂະຫຍາຍໂດຍຜ່ານການອະທິ ບາຍ ການສາທິດ ແລະ ຫຼັກຖານຕໍ່ໄປນີ້.

ຫຼັກການ ທີ 1: ເປັນເຈົ້າຂອງຜົນໄດ້ຮັບດ້ານ ຄວາມປອດໄພຂອງລູກຄ້າ

ຄຳອະທິບາຍ

ແນວປະຕິບັດທີ່ດີທີ່ສຸດໃນປັດຈຸບັນກຳນົດວ່າໃຫ້ຜູ້ຜະລິດຊອັບແວລົງທຶນໃນຄວາມພະຍາຍາມດ້ານຄວາມປອດໄພຂອງຜະລິດຕະພັນທີ່ ປະກອບມີ **ການເຮັດໃຫ້ ແອັບພລິເຄຊັນເຂັ້ມແຂງຂຶ້ນ ຄຸນສົມບັດຂອງແອັບພລິເຄຊັນ,** ແລະ ແອັບພລິເຄຊັນ **ຄ່າເລີ່ມຕົ້ນ ການຕັ້ງຄ່າ.**

ຜູ້ຜະລິດຊອັບແວຈຳເປັນຕ້ອງໄດ້ໃຊ້ **ການເສີມຄວາມແຂງແຮງຂອງແອັບພລິເຄຊັນ** ໂດຍໃຊ້ຂະບວນການ ແລະ ເທັກໂນໂລຍີທີ່ເພີ່ມ ຄ່າໃຊ້ຈ່າຍໃຫ້ກັບຜູ້ກະທຳທີ່ເປັນອັນຕະລາຍທີ່ຢາກປະນີປະນອມແອັບພລິເຄຊັນ. ໂປຣໂຕຄອນ ແລະ ຂັ້ນຕອນການເພີ້ມຄວາມແຂງຕົວ ຂອງແອັບພລິເຄຊັນ ຊ່ວຍໃຫ້ຜະລິດຕະພັນຕ້ານທານກັບການໂຈມຕີຈາກຜູ້ປະສົງຮ້າຍທີ່ສະຫຼາດ. ຄຳສັບຕ່າງໆເຊັ່ນ ການແຂງຕົວ, ຄວາມປອດໄພຂອງຜະລິດຕະພັນ ແລະ ຄວາມຢືດຢຸ່ນແມ່ນກ່ຽວຂ້ອງຢ່າງໃກ້ຊິດກັບຄຸນນະພາບຂອງຜະລິດຕະພັນ. ແນວຄິດກໍ ແມ່ນວ່າຄວາມປອດໄພຕ້ອງໄດ້ຮັບການ "ຝັງເລິກ" ແລະ ບໍ່ແມ່ນ "ຍຶດຕິດ." [1] ດ້ວຍການຝັງເລິກຄວາມປອດໄພ ຜູ້ຜະລິດຊອັບແວ ບໍ່ພຽງແຕ່ ສາມາດເພີ່ມຄວາມປອດໄພຂອງລູກຄ້າຂອງເຂົາເຈົ້າເທົ່ານັ້ນ ແຕ່ຍັງເພີ່ມຄຸນນະ ພາບຂອງຜະລິດຕະພັນຂອງພວກເຂົາອີກ ດ້ວຍ. ຍຸດທະວິທີຕົວຢ່າງລວມມີການຮັບປະກັນການປ້ອນຂໍ້ມູນຂອງຜູ້ໃຊ້ຖືກກວດສອບ ແລະ ຖືກອະນາໄມ ແລະ ບໍ່ໄດ້ໃສ່ລະຫັດໂດຍ ກົງ (ເຊັ່ນ ໂດຍໃຊ້ການສອບຖາມ ແບບພາລາມິເຕີແທນ), ການໃຊ້ພາສາການຂຽນໂປຣແກຣມທີ່ປອດໄພສຳລັບ ໜ່ວຍຄວາມຈຳ, ການ ຈັດການວົງຈອນຊີວິດການພັດທະນາຊອັບແວ (SDLC) ທີ່ເຄັ່ງຄັດ ແລະ ການໃຊ້ຮາດແວ - ການຄຸ້ມຄອງກະແຈການເຂົ້າລະຫັດທີ່ໄດ້ ຮັບການສະໜັບສະໜູນ.

ແອັບພລິເຄຊັນຕ້ອງຮອງຮັບ **ຄຸນສົມບັດແອັບພລິເຄຊັນ** ທີ່ກ່ຽວຂ້ອງ ກັບຄວາມປອດໄພທາງໄຊເບີ. ບາງຄັ້ງເອີ້ນວ່າ "ຄວາມສາມາດ," ຄຸນສົມບັດເຫຼົ່ານີ້ຈະຂະຫຍາຍການເຮັດວຽກ ຂອງຜະລິດຕະພັນຫຼືການບໍລິການໃນວິທີການທີ່ຊ່ວຍຮັກສາຫຼືເພີ່ມມາດຕາການ ຄວາມປອດໄພຂອງລູກຄ້າ.

ຕົວຢ່າງຄຸນສົມບັດທີ່ກ່ຽວຂ້ອງກັບຄວາມປອດໄພລວມມີການສະໜັບສະໜູນຄວາມປອດໄພຊັ້ນການຂົນສົ່ງ (Transport Layer Security –(TLS) ສຳລັບການເຊື່ອມຕໍ່ເຄືອຂ່າຍທັງໝົດ ການສະໜັບສະໜູນການເຂົ້າສູ່ລະບົບຄັ້ງດຽວ (SSO), ການສະໜັບສະໜູນ ການພິສູດຢືນຢັນແບບ ຫຼາຍປັດໃຈ (MFA), ການກວດສອບເຫດການຄວາມປອດໄພ, ການຄວບຄຸມ ການເຂົ້າເຖິງໂດຍອີງໃສ່ບົດບາດ (RBAC), ແລະ ການຄວບຄຸມການເຂົ້າເຖິງ ໂດຍອີງໃສ່ຄຸນລັກສະນະ (ABAC).

ບາງຄຸນສົມບັດຂອງຜະລິດຕະພັນເຫຼົ່ານີ້ແມ່ນສາມາດກຳນົດຄ່າໄດ້ ຊ່ວຍໃຫ້ ລູກຄ້າສາມາດເຊື່ອມໂຍງຜະລິດຕະພັນເຂົ້າກັບສະພາບ ແວດລ້ອມ ແລະ ຂັ້ນຕອນການເຮັດວຽກທີ່ມີຢູ່ຂອງເຂົາເຈົ້າໄດ້ງ່າຍຂຶ້ນ. ການກຳນົດຄ່າເຫຼົ່ານັ້ນໝາຍຄວາມວ່າແອັບພລິເຄຊັນຕ້ອງມີ **ການ ຕັ້ງຄ່າເລີ່ມຕົ້ນ** ໄວ້ຈົນກວ່າລູກຄ້າຈະກຳນົດຄ່າ ການຕັ້ງຄ່າເລີ່ມຕົ້ນເຫຼົ່ານັ້ນຈຳເປັນຕ້ອງຖືກຕັ້ງຄ່າຢ່າງປອດໄພ "ທັນທີ" ເພື່ອໃຫ້ລູກຄ້າໃຊ້ ຊັບພະຍາກອນໜ້ອຍລົງເພື່ອເຮັດໃຫ້ຜະລິດຕະພັນເທັກໂນໂລຢີຂອງພວກເຂົາມີຄວາມປອດໄພຫຼາຍຂຶ້ນ.

ແຕ່ລະອົງປະກອບເຫຼົ່ານີ້ ເຊັ່ນ ການແຂງຕົວຂອງແອັບພລິເຄຊັນ, ລັກສະນະຄວາມປອດໄພຂອງແອັບພລິເຄຊັນ ແລະ ການຕັ້ງຄ່າເລີ່ມຕົ້ນ ຂອງແອັບພລິເຄຊັນ - ມີບົດບາດໃນການຮັກສາຄວາມປອດໄພຂອງ ແອັບພລິເຄຊັນ ແລະ ຜົນການຮັກສາຄວາມປອດໄພຂອງລູກຄ້າ. ຜູ້ ຜະລິດຊອັບແວຄວນຄິດກ່ຽວກັບແຕ່ລະອົງປະກອບເຫຼົ່ານີ້ ແລະ ເບິ່ງວ່າອົງປະກອບເຫຼົ່ານີ້ກ່ຽວຂ້ອງກັນຢ່າງໃດ. ຜູ້ຜະລິດຄວນຄິດຫຼາຍກວ່າ ພຽງແຕ່ການລົງທຶນເພື່ອລວມເອົາອົງປະກອບເຫຼົ່ານີ້ເຂົ້າໃນຜະລິດຕະພັນຂອງຕົນ. ຜູ້ຜະລິດຄວນກ້າວໄປອີກຂັ້ນໜຶ່ງ ແລະ ພິຈາລະນາວ່າ ອົງປະກອບເຫຼົ່ານັ້ນປ່ຽນແປງທ່າທາງຄວາມປອດໄພທີ່ແທ້ຈິງຂອງລູກຄ້າຂອງພວກເຂົາແນວໃດ ດີຂຶ້ນ ຫຼື ຮ້າຍແຮງກວ່າເກົ່າ.

ຜູ້ຜະລິດຄວນຖືຄວາມເປັນເຈົ້າຂອງຜົນໄດ້ຮັບດ້ານຄວາມປອດໄພຂອງລູກຄ້າແທນທີ່ຈະວັດແທກຜົນຂອງຕົນເອງຈາກຄວາມພະຍາຍາມ ແລະ ການລົງທຶນພຽງ ຢ່າງດຽວ. ຄວາມຮັບຜິດຊອບຄວນຈະຖືກວາງໄວ້ຕົ້ນທາງກັບຜູ້ຜະລິດ ບ່ອນທີ່ມັນມີຄວາມເປັນໄປໄດ້ຫຼາຍທີ່ສຸດໃນ ການຫຼຸດຜ່ອນໂອກາດຂອງການປະນີປະນອມ.

ແຕ່ໜ້າເສັຍດາຍ ທີ່ມື້ນີ້ບໍ່ເປັນເຊັ່ນນັ້ນ. ຜູ້ຜະລິດຈຳນວນຫຼາຍເກີນໄປວາງພາລະດ້ານຄວາມປອດໄພໄວ້ກັບລູກຄ້າຫຼາຍກວ່າການລົງທຶນ ໃນ **ການເຮັດໃຫ້ແອັບພລິເຄຊັນມີຄວາມເຂັ້ມແຂງ ຢ່າງຄົບຖ້ວນ.** ຕົວຢ່າງ ເມື່ອຜູ້ຜະລິດແກ້ໄຂຄວາມສ່ຽງຈຸດໜຶ່ງ ພວກເຮົາມັກຈະເຫັນ ຊ່ອງໂຫວ່ທີ່ຄ້າຍຄືກັນຖືກເປີດເຜີຍຍ້ອນວ່າຊ່ອງໂຫວ່ດັງກ່າວລະບຸເຖິງອາການຫຼາຍກວ່າແທນທີ່ ຈະເປັນຕົ້ນເຫດອັນແທ້ຈິງຂອງຂໍ້ບົກຜ່ອງ ນັ້ນ. ຜະລິດຕະພັນອາດຈະນຳໃຊ້ການຫຼຸດຜ່ອນທີ່ແຕກຕ່າງກັນໃນພາກສ່ວນ ຕ່າງໆຂອງຖານລະຫັດສຳລັບຊ່ອງໂຫວ່ປະເພດດຽວກັນ. ໃນ ກໍລະນີນີ້, ຫຼັງຈາກທີ່ຜູ້ຜະລິດໄດ້ແກ້ໄຂຊ່ອງໂຫວ່ໃນການອະນາໄມ ອິນພຸດແລ້ວ, ນັກວິໄຈ ຫຼື ຜູ້ໂຈມຕີໄດ້ພົບເສັ້ນທາງລະຫັດທີ່ບໍ່ໄດ້ຮັບຜົນ ປະໂຫຍດຈາກການອະນາໄມອິນພຸດທີ່ໄດ້ຮັບການປັບປຸງ. ຜູ້ຜະລິດໄດ້ນຳໃຊ້ການແກ້ໄຂເທື່ອລະອັນ ແທນທີ່ຈະລວມເອົາຖານລະຫັດ ເພື່ອ ກຳຈັດກຸ່ມຊ່ອງໂຫວ່ໃນລະດັບນັ້ນທົ່ວແອັບພລິເຄຊັນທັງໝົດ.

ຄຸນສົມບັດຂອງແອັບພລິເຄຊັນ ສາມາດສ້າງທັງປະໂຫຍດ ແລະ ຄວາມສ່ຽງໃຫ້ແກ່ລູກຄ້າ. ຄຸນນະສົມບັດທີ່ຊ່ວຍໃຫ້ສາມາດລວມຈຸດເຂົ້າກັບ ລະບົບ ແລະ ເວີຊັ່ນພາຍນອກຈຳນວນຫຼາຍ ສາມາດເພີ່ມມູນຄ່າຂອງຜະລິດຕະພັນໄດ້ຢ່າງຫຼວງຫຼາຍ. ແລະ ການສະໜັບສະໜູນຄຸນສົມບັດ ຕ່າງໆທີ່ບໍ່ມີການວາງແຜນການເລີກໃຊ້ ເຊັ່ນ ໂປຣໂຕຄອນເຄືອຂ່າຍ ອາດເຮັດໃຫ້ລູກຄ້າມີຄວາມສ່ຽງໄດ້ຖ້າ ພວກເຂົາ ຂາດຄວາມເຂົ້າໃຈ ກ່ຽວກັບຜົນສະທ້ອນຂອງການນຳໃຊ້ຄຸນ ສົມບັດນັ້ນຢ່າງຕໍ່ເນື່ອງ. ຕົວຢ່າງ, ບາງຜະລິດຕະພັນຍັງສືບຕໍ່ໃຊ້ໂປຣໂຕຄອນເຄືອຂ່າຍທີ່ມີຕົ້ນ ກຳເນີດໃນຊຸມປີ 1990 ຫຼື 2000 ແລະ ປະຈຸບັນຮູ້ວ່າບໍ່ປອດໄພ. ມີຫຼາຍປັດໃຈທີ່ອາດເຮັດໃຫ້ລູກຄ້າອັບເກຣດ ແລະ ນຳໃຊ້ມາດຕະການ ຄວາມປອດໄພທັນສະໄໝໄດ້ໄວເທົ່າໃດ. ພວກເຂົາອາດຈະໃຊ້ຜະລິດຕະພັນທີ່ປະສົມປະສານກັບສ່ວນທີ່ເຫຼືອຂອງເຄືອຂ່າຍຂອງອົງກອນ, ແຕ່ ຂາດມາດຕະການຮັກສາຄວາມປອດໄພ ທີ່ທັນສະໄຫມເຮັດໃຫ້ທີມງານ ໄອທີ ບໍ່ສາມາດປັບປຸງໃຫ້ທັນສະໄໝໄດ້. ຢ່າງໃດກໍຕາມ, ຜູ້ຜະລິດຊ ອັບແວສາມາດປະກອບຮູບແບບເຫຼົ່ານີ້ເຂົ້າໃນຂະບວນການວາງແຜນຂອງພວກເຂົາເພື່ອຊຸກຍູ້ໃຫ້ລູກຄ້າຢູ່ໃນປະຈຸບັນໄດ້.

ການຕັ້ງຄ່າເລີ່ມຕົ້ນຂອງແອັບພລິເຄຊັນ ເປັນພື້ນທີ່ເພີ່ມຄວາມສ່ຽງທີ່ອາດເກີດຂຶ້ນສຳລັບລູກຄ້າ. ຜູ້ຜະລິດມັກຈະເລືອກການຕັ້ງຄ່າເລີ່ມຕົ້ນ ບາງຢ່າງ ເຮັດໃຫ້ງ່າຍຂຶ້ນສຳລັບລູກຄ້າທີ່ຈະໃຊ້ຄຸນສົມບັດຂອງແອັບພລິເຄຊັນທີ່ເຂົາເຈົ້າຕ້ອງການ. ຂໍ້ເສັຍແມ່ນວ່າແນວທາງປະຕິບັດນີ້ເພີ່ມ ພື້ນທີ່ການໂຈມຕີໃຫ້ກັບລູກຄ້າທີ່ອາດຈະບໍ່ຕ້ອງ ການຄຸນສົມບັດ ແລະ ໂປຣໂຕຄອນບາງຢ່າງທີ່ຖືກເປີດໃຊ້ໂດຍຄ່າເລີ່ມຕົ້ນ. ນອກຈາກນີ້ ການຄວບຄຸມຄວາມປອດໄພຫຼາຍຢ່າງຈະຖືກປິດໃຊ້ວຽກງານຕາມຄ່າເລີ່ມຕົ້ນ ຫຼື ກຳນົດໃຫ້ລູກຄ້າຕ້ອງໃຊ້ເວລາໃນກຳນົດການຕັ້ງຄ່າຂອງ ເຂົາເຈົ້າເພື່ອເພີ່ມຄວາມປອດໄພ. ການສ້າງແບບຈຳລອງໄພຂົ່ມຂູ່ທີ່ຊັດເຈນແມ່ນກົນລະຍຸດທີ່ອາດຈະຊ່ວຍແຈ້ງການຕັດສິນໃຈວ່າລັກສະນະໃດ ຄວນຈະຖືກເປີດໃຊ້ເປັນຄ່າເລີ່ມຕົ້ນ ຫຼື ການຕັ້ງຄ່າໃດທີ່ຕ້ອງການເພື່ອໃຫ້ປອດໄພໂດຍຄ່າເລີ່ມຕົ້ນ. ຍຸດທະວິທີອີກຢ່າງໜຶ່ງຄືການກວດສອບ ວິທີການເຮັດໃຫ້ຜູ້ດູແລລະບົບ ສາມາດຄົ້ນພົບຄຸນສົມບັດຕ່າງໆໄດ້ຫຼາຍຂຶ້ນ.

ຜູ້ຜະລິດບາງຄົນຈັດສົ່ງຜະລິດຕະພັນທີ່ມີຄ່າເລີ່ມຕົ້ນທີ່ອາດສ້າງຄວາມສ່ຽງຕໍ່ລູກຄ້າບາງຄົນ ຫຼື ທັງໝົດຂອງພວກເຂົາໄດ້. ແທນທີ່ຈະຕັ້ງຄ່າເລີ່ມຕົ້ນທີ່ປອດໄພກວ່າ ພວກເຂົາມັກຈະເລືອກຜະລິດ **ຄູ່ມືການແຂງຕົວ** ທີ່ລູກຄ້າຕ້ອງດຳເນີນການດ້ວຍຄ່າໃຊ້ຈ່າຍຂອງຕົນເອງ. ຄູ່ມືການແຂງຕົວປະສົບບັນຫາທົ່ວໄປຫຼາຍຢ່າງ. ບາງຄູ່ມືການແຂງຕົວບາງອັນແມ່ນຍາກທີ່ຈະຊອກຫາໄດ້ຍາກ ແລະ ບໍ່ໄດ້ຮັບການສະໜັບສະໜູນທີ່ດີ. ສ່ວນອື່ນໆແມ່ນມີຄວາມຊັບຊ້ອນໃນການປະຕິບັດ ບາງຄັ້ງຕ້ອງມີການການພັດທະນາຊອັບແວເພື່ອຂຽນໂມດູນການຂະຫຍາຍ. ຢ່າງໃດກໍຕາມ, ຄົນອື່ນຖືວ່າຜູ້ອ່ານມີປະສົບການດ້ານຄວາມປອດໄພທາງໄຊເບີຢ່າງກວ້າງ ຂວາງເພື່ອທຳຄວາມເຂົ້າໃຈວິທີການຕ່າງໆໃນການປ່ຽນແປງພື້ນທີ່ການໂຈມຕີ. ຜູ້ປະຕິບັດງານທີ່ມີຄວາມເຂົ້າໃຈບໍ່ຄົບຖ້ວນກ່ຽວກັບວິທີການເຮັດວຽກຂອງຜູ້ໂຈມຕີອາດຈະລົ້ມເຫຼວໃນການດຳເນີນການ ຕາມຄຳແນະນຳການແຂງຕົວຢ່າງຖືກຕ້ອງ ໂດຍສະເພາະຖ້າຄຳແນະນຳບໍ່ເຮັດໃຫ້ການແລກປ່ຽນຊັດເຈນ. ນອກຈາກນັ້ນ, ຄູ່ມືການແຂງຕົວທັງໝົດນັ້ນບໍ່ແມ່ນຂຽນໂດຍວິສະວະກອນທີ່ມີຄວາມຄຸ້ນເຄີຍກັບຍຸດທະວິທີ ແລະ ເສດຖະກິດຂອງຜູ້ໂຈມຕີ ເຮັດໃຫ້ພວກເຂົາສ້າງຄູ່ມືການແຂງຕົວທີ່ບໍ່ມີປະສິດຕິຜົນ ເຖິງແມ່ນວ່າຈະປະຕິບັດຢ່າງຊື່ສັດກໍຕາມ. ລູກຄ້າຫຼາຍລ້ານຄົນມີໜ້າທີ່ຮັບຜິດຊອບໃນການປັບປຸງຫຼາຍໆຕົວຢ່າງຂອງຊອັບແວ ຫຼື ລະບົບ ຊຶ່ງມັກຈະຢູ່ໃນສະພາບແວດລ້ອມທີ່ມີຊັບພະຍາກອນຈຳກັດ. ການອີງໃສ່ຄູ່ມືການແຂງຕົວພຽງແຕ່ບໍ່ໄດ້ປັບຂະໜາດ.

ການຕັ້ງຄ່າຂອງແອັບພລິເຄຊັນຄວນໄດ້ຮັບການປະເມີນຢ່າງຕໍ່ເນື່ອງວ່າການຕັ້ງຄ່ານັ້ນແມ່ນເປັນຄ່າເລີ່ມຕົ້ນ ຫຼື ຕັ້ງຄ່າໂດຍລູກຄ້າ, ໂດຍທຽບກັບຄວາມເຂົ້າໃຈໃນປັດຈຸບັນຂອງຜູ້ຜະລິດໃນປັດຈຸບັນກ່ຽວກັບພາບລວມໄພຂົ່ມຂູ່. ແອັບພລິເຄຊັ່ນຄວນຈະເຮັດໂດຍມີຕົວຊີ້ວັດທີ່ຊັດເຈນກ່ຽວກັບຄວາມສ່ຽງທີ່ອາດຈະເກີດຂຶ້ນຈາກການຕັ້ງຄ່າເຫຼົ່ານັ້ນ ແລະ ຄວນເຮັດໃຫ້ຕົວຊີ້ວັດເຫຼົ່ານັ້ນຮູ້ຈັກ. ເຊັ່ນກັນກັບລົດທີ່ທັນສະໄໝ ທີ່ມີຕົວຊີ້ວັດກ່ຽວກັບສາຍແອວນິລະໄພ ແລະ ສະແດງຕົວຊີ້ວັດນັ້ນໂດຍການສົ່ງສຽງເຕືອນໄພຖ້າທ່ານພະຍາຍາມຂັບລົດໂດຍບໍ່ຄາດສາຍແອວນັ້ນ, ຊອັບແວຄວນສະແດງຕົວຊີ້ວັດກ່ຽວກັບຄວາມປອດໄພຂອງລະບົບ. ຖ້າແອັບພລິເຄຊັນຖືກຕັ້ງຄ່າເພື່ອບໍ່ຕ້ອງການ MFA ສຳລັບບັນຊີຜູ້ດູແລລະບົບ ຄວນຈະເຮັດໃຫ້ຜູ້ດູແລລະບົບຮັບຮູ້ເປັນປະຈຳວ່າພວກເຂົາ ແລະ ອົງກອນທັງໝົດຂອງພວກເຂົາຕົກຢູ່ໃນອັນຕະລາຍຖ້າພວກເຂົາບໍ່ຕັ້ງຄ່າ MFA. ນອກຈາກນັ້ນ, ຖ້າແອັບພລິເຄຊັນຖືກຕັ້ງຄ່າເພື່ອສະໜັບສະໜູນໂປຣໂຕຄອນລຸ້ນເກົ່າທີ່ຮູ້ຈັກວ່າມີການໃຊ້ການເຂົ້າລະຫັດທີ່ບໍ່ມີປະສິດທິພາບ, ແອັບພລິເຄຊັນຄວນແຈ້ງໃຫ້ຜູ້ດູແລລະບົບຊາບຢ່າງຊັດເຈນເປັນປະຈຳວ່າອົງກອນກຳລັງຕົກຢູ່ໃນອັນຕະລາຍ ແລະ ຈັດຫາແຫຼ່ງຂໍ້ມູນ ເພື່ອແກ້ໄຂສະຖານະການ. ພວກເຮົາຂໍແນະນຳໃຫ້ຜູ້ຜະລິດດຳເນີນການກະຕຸ້ນຕາມປົກກະຕິທີ່ມີຢູ່ໃນຜະລິດຕະພັນແທນທີ່ຈະອີງໃສ່ຜູ້ດູແລລະບົບເພື່ອໃຫ້ມີເວລາ ຄວາມຊຳນານ ແລະ ຄວາມຮັບຮູ້ທີ່ຈະຕີຄວາມໝາຍຄູ່ມືການແຂງຕົວ. ເຫັນໄດ້ຢ່າງຈະແຈ້ງວ່າມີໂອກາດສຳລັບນະວັດຕະກຳເພື່ອສ້າງດຸ່ນດ່ຽງລະຫວ່າງການພິຈາ ລະນາດ້ານຄວາມປອດໄພ ແລະ ການນຳໃຊ້.

ແຕ່ລະອົງປະກອບຂ້າງເທິງນີ້ສ້າງສະຖານະການທີ່ບໍ່ສາມາດແກ້ໄຂໄດ້ທີ່ລູກຄ້າຕ້ອງການຄົ້ນຄ້ວາ ລະດົມທຶນ ຊື້ ພະນັກງານ ນຳໃຊ້ ແລະ ຕິດຕາມກວດກາເພີ່ມເຕີມ **ຜະລິດຕະພັນຮັກສາຄວາມປອດໄພ** ເພື່ອຫຼຸດຜ່ອນໂອກາດທີ່ຈະເກີດການປະນີປະນອມ. ໂດຍທົ່ວໄປແລ້ວ ອົງກອນຂະໜາດນ້ອຍ ແລະ ຂະໜາດກາງ (SMOs) ບໍ່ສາມາດອຳນວຍຄວາມສະດວກໃຫ້ແກ່ທາງເລືອກເຫຼົ່ານີ້ໄດ້. ພວກເຂົາປະເຊີນກັບການຂາດແຄນຄວາມຊຳນານ, ເງິນທຶນ ແລະ ເວລາທີ່ເກັບພາສີແບນວິດ ແລະ ການເຮັດວຽກງານ ບັງຄັບໃຫ້ການຮັກສາຄວາມປອດໄພມີລຳດັບຕ່ຳ ແລະ ໂດຍລວມແລ້ວ ເຮັດໃຫ້ຄວາມສ່ຽງລວມເພີ່ມຂຶ້ນ. ໃນທາງກົງກັນຂ້າມ, ການລົງທຶນດ້ານຄວາມປອດໄພຂອງຜູ້ຜະລິດຈຳນວນໜ້ອຍກໍຈະຂະຫຍາຍຕົວຫຼາຍຂຶ້ນ. ປະໂຫຍກທົ່ວໄປທີ່ສະຫຼຸບບັນຫາແມ່ນວ່າອຸດສາຫະກຳຊອັບແວຕ້ອງການຜະລິດຕະພັນທີ່ປອດໄພຫຼາຍຂຶ້ນ ບໍ່ແມ່ນຜະລິດຕະພັນປອດໄພຫຼາຍ. ຜູ້ຜະລິດຊອັບແວຄວນເປັນຜູ້ນຳການປ່ຽນແປງດັ່ງກ່າວ.

> ***ອຸດສາຫະກຳຊອັບແວຕ້ອງການຜະລິດຕະພັນທີ່ປອດໄພຫຼາຍຂຶ້ນ,***
> ***ບໍ່ແມ່ນຜະລິດຕະພັນປດ້ານອດໄພຫຼາຍຂຶ້ນ.***
> ***ຜູ້ຜະລິດຊອັບແວຄວນເປັນຜູ້ນຳ ການປ່ຽນແປງດັ່ງກ່າວ.***

ມື້ນີ້, ບາງຄັ້ງພວກເຮົາອ່ານຄຳຄິດເຫັນຈາກຜູ້ຜະລິດທີ່ອະທິບາຍວ່າລູກຄ້າຖືກໂຈມຕີເນື່ອງຈາກການບໍ່ເປີດໃຊ້ຄຸນນະສົມບັດຄວາມປອດໄພ ໂດຍສະເພາະ ຫຼື ປະຕິບັດຕາມຄຳແນະນຳການແຂງຕົວໂດຍສະເພາະ. ແທນທີ່ ຫຼັງຈາກການປະນີປະນອມ, ຜູ້ຜະລິດຄວນອະທິບາຍວ່າຄຸນສົມບັດ ດ້ານຄວາມປອດໄພສະເພາະໃດໜຶ່ງ ຫຼື ຄຳແນະນຳການແຂງຕົວໂດຍສະເພາະຈະປ້ອງກັນການປະນີປະນອມ ຫຼື ບໍ່ ແລະ ພິຈາລະນາເຮັດໃຫ້ເປັນ ຄ່າເລີ່ມຕົ້ນໂດຍບໍ່ເສັຍຄ່າ. ໃນກໍລະນີທີ່ຜະລິດຕະພັນບໍ່ໄດ້ນັບການເສີມຄວາມເຂັ້ມແຂງ ພຽງພໍໃນຂັ້ນຕອນການອອກແບບ ແລະ ການໃຊ້ງານ, ຜູ້ຜະລິດຄວນອະທິບາຍວິທີການເຮັດວຽກເພື່ອກຳຈັດຊ່ອງໂຫວ່ຂອງປະເພດດັ່ງກ່າວອອກຈາກສາຍຜະລິດຕະພັນຂອງຕົນ.

ຜູ້ຜະລິດຊອັບແວມີໜ້າທີ່ຮັບຜິດຊອບເພື່ອໃຫ້ແນ່ໃຈວ່າຜະລິດຕະພັນຂອງຕົນ ຖືກອອກແບບ ແລະ ພັດທະນາໂດຍຄຳນຶງເຖິງຄວາມປອດໄພ ເປັນລຳດັບຄວາມສຳຄັນ ດ້ວຍເຫດນີ້, ພວກເຂົາຄວນ **ວັດຜົນຕາມຈຸດປະສົງ** ຂອງຄວາມພະຍາຍາມຂອງຕົນໃນພາກສະໜາມ. ພວກເຮົາ ຮຽກຮ້ອງໃຫ້ຜູ້ຜະລິດບໍ່ພຽງແຕ່ສຸມໃສ່ຄວາມພະຍາຍາມພາຍໃນຂອງຕົນ, ແຕ່ໃຫ້ວັດແທກຢ່າງເປັນກາງ ແລະ ລາຍງານຜົນໄດ້ຮັບ ແລະ ປະສິດທິຜົນຂອງຄວາມພະຍາຍາມ ແລະ ການກຳນົດຄ່າຄວາມປອດໄພຂອງຜະລິດຕະພັນຢ່າງສະໝ່ຳສະເໝີ ແລະ ສ້າງວົງຈອນຕອບຮັບຄຳຄິດ ຄຳເຫັນທີ່ສ້າງການປ່ຽນແປງໃນ SDLC ທີ່ນຳໄປສູ່ການປັບປຸງທີ່ສາມາດວັດແທກຜົນໄດ້ໃນຄວາມປອດໄພຂອງລູກຄ້າ ແລະ ຜະລິດຕະພັນທີ່ ປອດໄພຍິ່ງຂຶ້ນ. ການລາຍງານຄວນປະກອບມີຂໍ້ມູນທີ່ບໍ່ລະບຸຊື່ທີ່ຊຸມຊົນການຄົ້ນຄວ້າທາງດ້ານວິຊາການ ແລະ ການວິໄຈດ້ານຄວາມປອດໄພສາ ມາດນຳໃຊ້ເພື່ອຕິດຕາມແນວໂນ້ມລະດັບສູງ ແລະ ວັດແທກຄວາມກ້າວໜ້າຂອງລະບົບນິເວດຢ່າງກວ້າງຂວາງ.

ສາທິດຫຼັກການນີ້

ຜູ້ຜະລິດຊອັບແວ ແລະ ການບໍລິການອອນລາຍຄວນຊອກຫາວິທີທີ່ຈະສະແດງໃຫ້ເຫັນຜົນສຳເລັດໃນການນຳຫຼັກການນີ້ໄປໃຊ້. ພວກເຂົາຄວນ ຊອກຫາຫຼັກຖານທີ່ເປັນສິນລະປະວັດຖຸເພື່ອໃຫ້ບຸກຄົນພາຍນອກກວດສອບ. ບໍ່ມີສິ່ງປະດິດໃດໆໂດຍຕົວມັນເອງທີ່ຈະພິສູດວ່າຜູ້ຜະລິດ ກຳລັງໃຊ້ໂປຣແກຣມການອອກແບບການຮັກສາຄວາມທີ່ປອດໄພ, ແຕ່ໂດຍການຈັດຕຽມສິ່ງປະດິດຕ່າງໆ ພວກເຂົາຈະສ້າງກໍລະນີຂອງຄວາມ ມຸ່ງໝັ້ນຂອງຜູ້ຜະລິດໃນການພັດທະນາຜະລິດຕະພັນທີ່ປອດໄພ. ວິທີການນີ້ແມ່ນຢູ່ໃນຈິດວິນຍານຂອງ "ການສະແດງໃຫ້ເຫັນ, ຫຼາຍກ່ວາການ ບອກເລົ່າ"

ເພື່ອສາທິດຫຼັກການນີ້, ຜູ້ຜະລິດຊອັບແວຄວນພິຈາລະນາຂັ້ນຕອນຕ່າງໆດັ່ງໃນບັນຊີລາຍການຕໍ່ໄປນີ້. ອົງກອນຜູ້ຂຽນຮັບຮູ້ວ່າຜູ້ຜະລິດຊອັບ ແວຈຳນວນໜ້ອຍຈະສາມາດນຳເອົາແນວປະຕິບັດເຫຼົ່ານີ້ໄປໃຊ້ໄດ້ທັນທີ ແລະ ຜະລິດສິ່ງປະດິດທີ່ສອດຄ່ອງກັນໃນຕອນເລີ່ມຕົ້ນຂອງເສັ້ນທາງ ການອອກແບບໂດຍຄວາມປອດໄພ. ນອກຈາກນັ້ນ, ຜູ້ຜະລິດຊອັບແວຈະຕ້ອງຈັດລຳດັບຄວາມສຳຄັນຂອງບັນຊີລາຍຊື່ນີ້ໂດຍອີງຕາມວິທີການ ລູກຄ້ານຳໃຊ້ຜະລິດຕະພັນໃນພາກສະໜາມເພື່ອໃຫ້ບັນລຸຜົນປະໂຫຍດດ້ານຄວາມປອດໄພທີ່ໃຫຍ່ທີ່ສຸດ.

ແນວປະຕິບັດ ຄວາມປອດໄພໂດຍຄ່າເລີ້ມຕົ້ນ

1. **ກຳຈັດລະຫັດຜ່ານໂດຍເລີ່ມຕົ້ນ.** ລະຫັດຜ່ານເລີ່ມຕົ້ນຍັງສືບຕໍ່ເປັນສາເຫດຂອງການໂຈມຕີຫຼາຍຄັ້ງໃນແຕ່ລະປີ. ການມຸ່ງໝັ້ນທີ່ຈະກຳຈັດບັນຫາຊ້ຳເຮື້ອນີ້ຈະປະຕິເສດການເຂົ້າເຖິງຜູ້ໂຈມຕີໄດ້ງ່າຍ. ເຊັ່ນດຽວກັນ, ຜູ້ຜະລິດຄວນພິຈາລະນາວ່າການໃຊ້ແນວທາງປະຕິບັດກ່ຽວກັບລະຫັດຜ່ານຄວນຖືກປະຕິບັດແນວໃດ, ເຊັ່ນຄວາມຍາວຂອງລະຫັດຜ່ານຂັ້ນຕ່ຳ ແລະ ການບໍ່ອະນຸຍາດໃຫ້ມີລະຫັດຜ່ານທີ່ຖືກລະເມີດ.

2. **ດຳເນີນການທົດສອບພາກສະໜາມ.** ເມື່ອເທັກໂນໂລຢີຍັງຄົງມີການພັດທະນາ ແລະ ມີຄວາມຊັບຊ້ອນຫຼາຍຂຶ້ນ, ຜູ້ຜະລິດຊອບແວຈຶ່ງມີຄວາມສຳຄັນຫຼາຍຂຶ້ນເລື້ອຍໆ ໃນການດຳເນີນການທົດສອບ ໂດຍຜູ້ໃຊ້ທີ່ເນັ້ນຄວາມປອດໄພເປັນຫຼັກເພື່ອເຂົ້າໃຈມາດຕະການການຮັກສາຄວາມປອດໄພຂອງຜະລິດຕະພັນຂອງຕົນໃນພາກສະໜາມ. ຄືກັນກັບວິທີການຄົ້ນຄ້ວາຂອງຜູ້ໃຊ້ແຈ້ງຂໍ້ກຳນົດໃນການພັດທະນາຊອບແວ ຜູ້ຜະລິດຊອບແວຄວນເຮັດການຄົ້ນຄວ້າຜູ້ໃຊ້ທີ່ເນັ້ນຄວາມປອດໄພເພື່ອເຂົ້າໃຈວ່າປະສົບການຂອງຜູ້ໃຊ້ດ້ານຄວາມປອດໄພ (UX) ສັ້ນລົງ. ໂດຍການສັງເກດເບິ່ງວິທີການທີ່ລູກຄ້ານຳມາໃຊ້ ແລະ ນຳໃຊ້ຜະລິດຕະພັນຂອງຕົນ ໃນສະພາບແວດລ້ອມທີ່ແທ້ຈິງ, ຜູ້ຜະລິດຊອບແວສາມາດໄດ້ຮັບຄວາມເຂົ້າໃຈທີ່ມີຄຸນຄ່າກ່ຽວກັບການນຳໃຊ້ ແລະ ປະສິດທິພາບຂອງຄຸນສົມບັດຄວາມປອດໄພ ແລະ ການຄວບຄຸມດ້ານຄວາມປອດໄພຂອງຕົນ ຂໍ້ມູນອັນເລິກເຊິ່ງເຫຼົ່ານີ້ສາມາດຊ່ວຍກຳນົດພື້ນທີ່ສຳລັບການປັບປຸງ ແລະ ປັບແຕ່ງຜະລິດຕະພັນຂອງພວກເຂົາເພື່ອຕອບສະໜອງຄວາມຕ້ອງການດ້ານຄວາມປອດໄພຂອງລູກຄ້າໄດ້ດີຍິ່ງຂຶ້ນ. ຕົວຢ່າງເຊັ່ນ ການທົດສອບພາກສະໜາມອາດຈະແນະນຳການປ່ຽນແປງໃນ ກະແສຂອງ UX ຄ່າເລີ່ມຕົ້ນ ການແຈ້ງເຕືອນ ແລະ ການຕິດຕາມກວດສອບ. ການທົດສອບພາກສະໜາມອາດຈະສະແດງໃຫ້ເຫັນວ່າການປັບປຸງທີ່ຜ່ານມາໃນການອອກແບບຂອງຜະລິດຕະພັນຫຼຸດຜ່ອນຄວາມໄວຂອງແຜ່ນຮັກສາຄວາມປອດໄພ, ຫຼຸດຜ່ອນຄວາມຜິດພາດໃນການຕັ້ງຄ່າ ແລະ ຫຼຸດຜ່ອນພື້ນທີ່ການບຸກໂຈມຕີໃຫ້ເຫຼືອໜ້ອຍທີ່ສຸດ.

ຜູ້ຜະລິດຄວນພິຈາລະນາດັ່ງຕໍ່ໄປນີ້:

- ລູກຄ້າປະຕິບັດຕາມຄຳແນະນຳການແຂງຕົວໄດ້ຢ່າງຖືກຕ້ອງບໍ?
- ຄຸນສົມບັດດ້ານຄວາມປອດໄພທີ່ມີຢູ່ແລ້ວຂອງຜະລິດຕະພັນປະຕິບັດໄດ້ຕາມທີ່ຄາດໄວ້ໃນພາກສະໜາມບໍ?
- ຄຸນສົມບັດເຫຼົ່ານັ້ນຕ້ານກັບການໂຈມຕີໃນໂລກແຫ່ງຄວາມເປັນຈິງໄດ້ແທ້ບໍ?
- ຄຸນສົມບັດໃດແດ່ທີ່ຈະຫຼຸດຄວາມເປັນໄປໄດ້ຂອງການປະນີປະນອມໄດ້ດີກວ່າ?

ໝາຍເຫດ: ເພື່ອໃຫ້ໄດ້ຮັບຄວາມເຂົ້າໃຈເລິກເຊິ່ງກ່ຽວກັບອົງປະກອບເຫຼົ່ານີ້, ຜູ້ຜະລິດຊອບແວອາດຈະຕ້ອງການທີ່ຈະຮ່ວມມືກັບລູກຄ້າເພື່ອດຳເນີນການເຝິກຊ້ອມຂອງທີມສີແດງເພື່ອເບິ່ງວ່າຜະລິດຕະພັນຕ້ານກັບການໂຈມຕີແນວໃດ. ການທົດສອບພາກສະໜາມເຫຼົ່ານີ້ອາດຈະເກີດຂຶ້ນຢູ່ສະຖານທີ່ຈິງຂອງລູກຄ້າ, ທາງອອນລາຍ ຫຼື ຜ່ານການກວດສອບທາງໄກ (telemetry) ຈາກແອັບພລິເຄຊັ່ນໃນລັກສະນະປົກປັກຮັກສາຄວາມເປັນສ່ວນຕົວ.

3. **ຫຼຸດຜ່ອນຂະໜາດຄູ່ມືການແຂງຕົວ.** ຜູ້ຜະລິດສາມາດປັບປຸງມາດຕາການ ການຮັກສາຄວາມປອດໄພຂອງລູກຄ້າໄດ້ໂດຍການປັບຕົວ ຫຼື ການກຳຈັດຄຳແນະນຳການແຂງຕົວຂອງຜະລິດຕະພັນ ແລະ ເນັ້ນໃສ່ມາດຕະການຄວາມປອດໄພທີ່ສຳຄັນທີ່ສຸດທີ່ລູກຄ້າຄວນຈັດລຳດັບຄວາມສຳຄັນໃນເວລານຳໃຊ້ຜະລິດຕະພັນຂອງເຂົາເຈົ້າ. ແທນທີ່ຈະເຮັດໃຫ້ລູກຄ້າລົ້ນຫຼາມດ້ວຍລາຍການມາດຕະການການຮັກສາຄວາມປອດໄພ ຜູ້ຜະລິດຄວນລະບຸຄວາມສ່ຽງດ້ານຄວາມປອດໄພສູງສຸດທີ່ຜະລິດຕະພັນຂອງເຂົາເຈົ້າມີຄວາມສ່ຽງ ແລະ ໃຫ້ຄຳແນະນຳທີ່ຊັດເຈນ ແລະ ຮັດກຸມກ່ຽວກັບວິທີການຫຼຸດຄວາມສ່ຽງເຫຼົ່ານີ້. ນອກຈາກນີ້, ຜູ້ຜະລິດຄວນຈັດຫາເຄື່ອງມື ແລະ ລະບົບອັດຕະໂນມັດໃຫ້ແກ່ລູກຄ້າທີ່ເຮັດໃຫ້ຂະບວນການປະຕິບັດການຄວບຄຸມຄວາມປອດໄພ ເຊັ່ນ ສະກຣິບທີ່ສາມາດຖືກນຳໃຊ້ໄດ້ງ່າຍໃນສະພາບແວດລ້ອມຂອງພວກເຂົາ. ເຄື່ອງມືເຫຼົ່ານີ້ ຄວນຈະສາມາດກວດສອບເພີ່ມເຕີມ ແລະ ສະແດງການປ່ຽນແປງທີ່ເກີດຂຶ້ນຈາກຂໍ້ມູນພື້ນຖານຕົ້ນສະບັບໄດ້ຢ່າງຊັດເຈນ. ດ້ວຍການປັບປຸງຄຳແນະນຳໃນການເສີມຄວາມແຂງຕົວ ແລະ ໃຫ້ລູກຄ້າມີເຄື່ອງມືທີ່ງ່າຍຕໍ່ການໃຊ້ ແລະ ລະບົບອັດຕະໂນມັດ ຜູ້ຜະລິດສາມາດຫຼຸດຜ່ອນພາລະຕໍ່ລູກຄ້າ ແລະ ຊ່ວຍໃຫ້ແນ່ໃຈວ່າຜະລິດຕະພັນຂອງຕົນຖືກນຳໄປໃຊ້ໃນລັກສະນະທີ່ປອດໄພ. ຍຸດທະວິທີອັນໜຶ່ງແມ່ນ ການພິຈາລະນາການປະຕິບັດຫຼັກການ Pareto ເພື່ອຫຼຸດຜ່ອນຈຳນວນຂັ້ນຕອນສຳລັບກໍລະນີທີ່ໃຊ້ທົ່ວໄປ (80%), ແລະ ຫຼັງຈາກນັ້ນໃຫ້ຄຳແນະນຳກ່ຽວກັບບໍລິບົດ ແລະ ເຄື່ອງມືສຳລັບສະຖານະການທົ່ວໄປທີ່ໜ້ອຍກ່ວາ (20%). ດ້ວຍວິທີນີ້, ຜູ້ຜະລິດຊອບແວຈະເຮັດໃຫ້ສິ່ງທີ່ຮຽກງ່າຍເປັນເລື່ອງງ່າຍ ແລະ ສິ່ງຍາກໆ ໃຫ້ເປັນໄປໄດ້. ການທົດສອບພາກສະໜາມຈະເປັນເຄື່ອງມືທີ່ມີປະສິດທິພາບໃນການວັດແທກວ່າລູກຄ້າຕ້ອງໃຊ້ເວລາດົນປານໃດໃນການຄົ້ນພົບ, ຄວາມເຂົ້າໃຈ ແລະ ປະຕິບັດຕາມຄຳແນະນຳໃນການເສີມຄວາມການແຂງຕົວ. ຜູ້ຜະລິດຄວນພິຈາລະນາວ່າຜະລິດຕະພັນສາມາດກະຕຸ້ນໃຫ້ຜູ້ດູແລລະບົບໃຫ້ດຳເນີນການພາຍໃນຕົວຜະລິດຕະພັນໄດ້ແນວໃດ ແທນທີ່ຈະອີງໃສ່ພວກເຂົາເພື່ອປະຕິບັດຕາມແນວທາງທີ່ເຂັ້ມງວດຍິ່ງຂຶ້ນ

4. **ຢ່າສະໜັບສະໜູນການໃຊ້ຄຸນສົມບັດເກົ່າທີ່ບໍ່ປອດໄພຢ່າງຈິງຈັງ.** ຈັດລະດັບຄວາມສຳຄັນຂອງການຮັກສາຄວາມປອດໄພຜ່ານເສັ້ນທາງການຍົກລະດັບທີ່ຊັດເຈນຕໍ່ກັບຄວາມເຂົ້າກັນໄດ້ແບບຍ້ອນຫຼັງ. ເຜີຍແຜ່ບລັອກໂພສ(blog) ທີ່ສະແດງໃຫ້ເຫັນການຮັບຮອງເອົາຄຸນສົມບັດ ແລະ ໂປຣໂຕຄອນທີ່ປອດໄພມາໃຊ້ ແລະ ເລີກໃຊ້ຄຸນສົມບັດທີ່ບໍ່ປອດໄພ ໂດຍການປະກາດ ເຊິ່ງອາດຈະມາຈາກພາຍໃນຜະລິດຕະພັນເອງ. ລູກຄ້າຈຳນວນຫຼວງຫຼາຍໄດ້ສະແດງໃຫ້ເຫັນວ່າພວກເຂົາຈະບໍ່ຮັກສາລະບົບຂອງເຂົາເຈົ້າໃຫ້ເປັນປະຈຸບັນດ້ວຍເຄືອຂ່າຍທີ່ທັນສະໄໝ ຂໍ້ມູນປະຈຳຕົວ ແລະ ຄຸນສົມບັດດ້ານຄວາມປອດໄພທີ່ສຳຄັນອື່ນໆ. ໃນບາງກໍລະນີ, ລູກຄ້າຢ້ານວ່າການທຳງານທີ່ມີຢູ່ແລ້ວຈະໃຊ້ງານບໍ່ໄດ້ເມື່ອມີການອັບເກຣດ. ດ້ວຍການອັບເກຣດແບບລາບລື່ນເທົ່າທີ່ເປັນໄປໄດ້ ລູກຄ້າມີແນວໂນ້ມທີ່ອາດຈະອັບເກຣດ ແລະ ໄດ້ຮັບການແກ້ໄຂດ້ານຄວາມປອດໄພເລື້ອຍໆ ແລະ ໄວຂຶ້ນ. ໂດຍການເຮັດໃຫ້ການອັບເກຣດແບບລາບລື່ນເທົ່າທີ່ເປັນໄປໄດ້, ລູກຄ້າອາດມີແນວໂນ້ມທີ່ຈະອັບເກຣດ ແລະ ໄດ້ຮັບການແກ້ໄຂຄວາມປອດໄພເລື້ອຍໆ ແລະ ໄວຂຶ້ນ. ຜູ້ຜະລິດຊອັບແວຄວນກະຕຸ້ນລູກຄ້າໄປຕາມເສັ້ນທາງອັບເກຣດເພື່ອຫຼຸດຜ່ອນຄວາມສ່ຽງຂອງລູກຄ້າ.

5. **ປະຕິບັດການແຈ້ງເຕືອນການດຶງດູດຄວາມສົນໃຈ.** ຄ້າຍກັບສຽງສາຍເຂັມຂັດນິລະໄພໃນລົດທີ່ສົ່ງສຽງດັງຢ່າງຕໍ່ເນື່ອງເມື່ອບໍ່ໄດ້ຮັດສາຍເຂັມຂັດນິລະໄພ, ຜູ້ຜະລິດຄວນໃຊ້ການແຈ້ງເຕືອນໃຫ້ທັນເວລາ ແລະ ຊ້ຳໆເມື່ອຜູ້ໃຊ້ ຫຼື ຜູ້ດູແລລະບົບຢູ່ໃນສະຖານະທີ່ບໍ່ປອດໄພຢ່າງແທ້ຈິງ ໂດຍເຕືອນຜູ້ດູແລລະບົບວ່າເຂົາເຈົ້າກຳລັງໃຊ້ ໂປຣໂຕຄອນທີ່ຖືກຍົກເລີກແລ້ວໃນສະພາບແວດລ້ອມ ແລະ ແນະນຳເສັ້ນທາງການອັບເກຣດ. ໃຊ້ການເຕືອນໃຫ້ທັນເວລາ ແລະ ຊ້ຳໆເມື່ອຜູ້ໃຊ້ ຫຼື ຜູ້ດູແລລະບົບ ຫຼື ການຕັ້ງຄ່າແອັບພລິ ເຄຊັນຢູ່ໃນສະຖານະທີ່ບໍ່ປອດໄພ. ແຈ້ງໃຫ້ຜູ້ດູແລລະບົບຊາບເຖິງໂໝດທີ່ບໍ່ປອດໄພເປັນປະຈຳ. ຄຸນສົມບັດເພີ່ມເຕີມສາມາດຮຽກຮ້ອງໃຫ້ຜູ້ດູແລລະບົບຂັ້ນສູງຮັບຮູ້ການບໍ່ມີ MFA ໃນບັນຊີຂອງຕົນໃນການເຂົ້າສູ່ລະບົບແຕ່ລະຄັ້ງ ຫຼື ແມ້ແຕ່ປິດການໃຊ້ງານຄຸນສົມບັດຫຼັກບາງຢ່າງຈົນກວ່າເຂົາເຈົ້າຈະເປີດໃຊ້ MFA. ມີພື້ນທີ່ໃຫ້ປະດິດສ້າງສິ່ງໃໝ່ໆເພື່ອໃຫ້ບັນລຸເປົ້າໝາຍເຫຼົ່ານີ້ ໃນຂະນະທີ່ບໍ່ໄດ້ສ້າງຄວາມເມື່ອຍລ້າໃນການແຈ້ງເຕືອນ.

6. **ສ້າງແມ່ແບບການຕັ້ງຄ່າທີ່ປອດໄພ.** ແມ່ແບບເຫຼົ່ານີ້ສາມາດຕັ້ງການຕັ້ງຄ່າບາງຢ່າງໄວ້ລ່ວງໜ້າຕໍ່ກັບການຕັ້ງຄ່າທີ່ປອດໄພ ໂດຍພິຈາລະນາຈາກຄວາມສ່ຽງທີ່ຍອມຮັບໄດ້ຂອງອົງກອນ. ໃນຂະນະທີ່ມັນອາດຈະງ່າຍດາຍເກີນໄປທີ່ຈະມີແມ່ແບບຄວາມປອດໄພຕ່ຳ / ກາງ / ສູງ ແຕ່ຕົວຢ່າງດັ່ງກ່າວນັ້ນສະແດງໃຫ້ເຫັນວ່າມີການຕັ້ງຄ່າໃດແດ່ທີ່ສາມາດຖືກອັບເກຣດເພື່ອຈັດການຄວາມສ່ຽງໃຫ້ອົງກອນໄດ້. ແມ່ແບບສາມາດໄດ້ຮັບການສະໜັບສະໜູນໂດຍຄູ່ມືການແຂງຕົວກ່ຽວກັບຄວາມສ່ຽງທີ່ຜູ້ຜະລິດໄດ້ລະບຸ.

ຫຼັກການໃນການພັດທະນາຜະລິດຕະພັນທີ່ປອດໄພ

1. **ຄວາມສອດຄ່ອງຂອງເອກະສານກັບກອບວຽກງານ SDLC ທີ່ປອດໄພ.** ກອບວຽກງານ SDLC ທີ່ປອດໄພໃຫ້ຈຸດປະສົງ ແລະ ຕົວຢ່າງສຳລັບບຸຄະລາກອນ , ຂະບວນການ ແລະ ເທັກໂນໂລຢີ. ພິຈາລະນາການເຜີຍແຜ່ຄຳອະທິບາຍໂດຍລະອຽດ ວ່າມີການໃຊ້ການຄວບຄຸມກອບວຽກງານ SDLC ທີ່ປອດໄພ ໃດແດ່ ແລະ ອະທິບາຍການຄວບຄຸມທາງເລືອກໃດໆທີ່ຖືກນຳ ໃຊ້. ພາຍໃນສະຫະລັດອະເມລິກາ ໃຫ້ພິຈາລະນານຳໃຊ້ ກອບ ວຽກ ການພັດທະນາຄວາມປອດໄພຂອງຊອັບແວ [NIST Secure Software Development Framework (SSDF)]. ໃນຂະນະທີ່ບໍ່ແມ່ນລາຍການກວດສອບ ແຕ່ SSDF "ອະທິບາຍຊຸດຂອງແນວປະຕິບັດພື້ນຖານທີ່ດີ ແລະ ເໝາະສົມສຳລັບການພັດທະນາຊອັບແວທີ່ປອດໄພ."

2. **ເອກະສານເປົ້າໝາຍການປະຕິບັດຄວາມປອດໄພທາງໄຊເບີ [Document Cybersecurity Performance Goals (CPG)] ຫຼື ຄວາມສອດຄ່ອງທີ່ ທຽບເທົ່າ.** ເມື່ອ ອົງກອນຢືນຢັນວ່າພວກເຂົາປະຕິບັດຕາມມາດຕະຖານ NIST SSDF, ພວກເຂົາກຳລັງຢືນຢັນວ່າ SDLC ຂອງຕົນ ໄດ້ຮັບການແຈ້ງບອກຈາກຫຼັກການທີ່ດີທີ່ສຸດທີ່ເຂົ້າໃຈກັນດີ. ຢ່າງໃດກໍຕາມ, ການມີ SDLC ທີ່ເຂັ້ມແຂງພຽງຢ່າງດຽວນັ້ນ ບໍ່ພຽງພໍສຳລັບພວກເຂົາ. ພວກເຂົາຍັງຈຳເປັນຕ້ອງປົກປ້ອງ ອົງກອນຂອງຕົນເອງ ແລະ ສະພາບແວດລ້ອມການພັດທະນາ ຂອງຕົນເອງຈາກຜູ້ບໍ່ປະສົງດີທີ່ເປັນອັນຕະລາຍທີ່ຈະພະຍາຍາມ ໝູນໃຊ້ຄຸນສົມບັດຄວາມປອດໄພຂອງຜະລິດຕະພັນ ໃນຂະນະທີ່ຍັງຢູ່ໃນການພັດທະນາ. ນີ້ບໍ່ແມ່ນການໂຈມຕີທາງທິດ ສະດີ ແຕ່ເປັນການໂຈມຕີທີ່ກໍ່ໃຫ້ເກີດຜົນກະທົບທາງລົບຕໍ່ ລູກຄ້າ ແລະ ໂດຍການຂະຫຍາຍຄວາມໝັ້ນຄົງຂອງຊາດ. ອົງກອນຄວນພິຈາລະນາການເຜີຍແຜ່ລາຍລະອຽດກ່ຽວກັບ ຄວາມສອດຄ່ອງຂອງອົງກອນຕາມ CISA CPGs, NIST ຂອບການເຮັດວຽກດ້ານຄວາມປອດໄພທາງໄຊເບີ(CSF), ຫຼື ກອບໂປຣແກຣມຄວາມປອດໄພທາງໄຊເບີອື່ນໆ.

3. **ການຈັດການຊ່ອງໂຫວ່.** ຜູ້ຜະລິດບາງຄົນມີໂປຣແກຣມຄຸ້ມ ຄອງຊ່ອງໂຫວ່ທີ່ເນັ້ນໃສ່ການແກ້ໄຂຊ່ອງໂຫວ່ທີ່ຄົ້ນພົບພາຍໃນ ຫຼື ພາຍນອກ ແລະ ອື່ນໆອີກເລັກນ້ອຍ. ໂປຣແກຣມທີ່ເຕີບໂຕ ເຕັມທີ່ຫຼາຍຂຶ້ນຈະລວມເອົາການວິເຄາະຊ່ອງໂຫວ່ທີ່ຂັບເຄື່ອນ ດ້ວຍຂໍ້ມູນອັນກວ້າງຂວາງ ແລະ ສາເຫດອັນແທ້ຈິງ ໂດຍດຳເນີນ ຕາມຂັ້ນຕອນເພື່ອລົບລ້າງຊ່ອງໂຫວ່ທັງໝົດຢ່າງເປັນລະບົບ[3]. ພວກເຂົາໃຊ້ໂປຣແກຣມຢ່າງເປັນທາງການກ່ຽວກັບການກຳນົດ ການວາງແຜນຄຸນນະພາບ ການຄວບຄຸມຄຸນນະພາບ, ການປັບປຸງຄຸນນະພາບ ແລະ ການວັດແທກຄຸນນະພາບ. ພວກເຂົາເບິ່ງ ວ່າການຈັດການຂໍ້ບົກພ່ອງເປັນບັນຫາເລື້ອງທຸລະກິດ, ບໍ່ແມ່ນພຽງແຕ່ ເລື່ອງຄວາມປອດໄພເທົ່ານັ້ນ. ບັນດາໂປຣແກຣມເຫຼົ່ານີ້ບໍ່ຄ້າຍຄືກັນໃນ ບາງທາງກັບໂປຣແກຣມຄຸນນະພາບ ແລະ ຄວາມປອດໄພໃນອຸດສາຫະ ກຳອື່ນໆ.

4. **ໃຊ້ຊອັບແວແຫຼ່ງເປີດ(open source software) ຢ່າງມີຄວາມຮັບຜິດຊອບ.** ເມື່ອ open source software ຖືກ ໃຊ້ ຈົ່ງຮັບຜິດຊອບໂດຍການກວດສອບແພັກເກັດ open source, ສົ່ງເສີມການປະກອບສ່ວນຂອງລະຫັດກັບຄືນສູ່ການເພິ່ງພາອາໄສ ແລະ ຊ່ວຍຮັກສາການພັດທະນາ ແລະ ການບຳລຸງຮັກສາອົງປະກອບທີ່ສຳ ຄັນ. ສຳລັບການອ້າງອີງ ກະຊວງເສດຖະກິດ ການຄ້າ ແລະ ອຸດສາຫະ ກຳຂອງຍີ່ປຸ່ນ (METI) ໄດ້ພິມເຜີຍແຜ່ "ການລວບລວມຕົວຢ່າງ ກໍລະນີກ່ຽວກັບວິທີການຄຸ້ມຄອງການນຳໃຊ້ OSS ແລະການຮັບປະກັນ ຄວາມປອດໄພຂອງມັນ."("Collection of Use Case Examples Regarding Management Methods for Utilizing OSS and Ensuring Its Security.")

5. **ໃຫ້ຄ່າເລີ່ມຕົ້ນທີ່ປອດໄພສຳລັບນັກພັດທະນາ.** ເຮັດໃຫ້ເສັ້ນທາງ ເລີ່ມຕົ້ນໃນລະຫວ່າງການພັດທະນາຊອັບແວເປັນເສັ້ນທາງທີ່ປອດໄພ ໂດຍການສະໜອງສິ່ງກໍ່ສ້າງທີ່ປອດໄພໃຫ້ກັບຜູ້ພັດທະນາ. ຕົວຢ່າງ ເຊັ່ນວ່າ ເນື່ອງຈາກຊ່ອງໂຫວ່ຂອງການແຊກ SQL ແຜ່ຫຼາຍທີ່ກໍ່ໃຫ້ເກີດ ອັນຕະລາຍໃນໂລກຂອງຄວາມເປັນຈິງ ກວດສອບໃຫ້ແນ່ໃຈວ່ານັກ ພັດທະນາໃຊ້ຫ້ອງສະໝຸດທີ່ມີການຮັກສາໄວ້ຢ່າງດີເພື່ອປ້ອງກັນຄວາມ ຊ່ອງໂຫວ່ຂອງປະເພດນັ້ນ. ເອີ້ນກັນອີກຢ່າງໜຶ່ງວ່າ “ຖະໜົນປູຢາງ” ຫຼື “ເສັ້ນທາງທີ່ມີແສງສະຫວ່າງດີ” ແນວປະຕິບັດນີ້ຮັບປະກັນທັງຄວາມໄວ ແລະ ຄວາມປອດໄພ ແລະ ຫຼຸດຜ່ອນຄວາມຜິດພາດຂອງມະນຸດ.

6. **ສົ່ງເສີມພະນັກງານພັດທະນາຊອັບແວທີ່ເຂົ້າໃຈຄວາມປອດໄພ.** ໃຫ້ ແນ່ໃຈວ່ານັກພັດທະນາຊອັບແວຂອງທ່ານເຂົ້າໃຈເລື້ອງຄວາມປອດໄພ ໂດຍການຝຶກອົບຮົມເຂົາເຈົ້າກ່ຽວກັບແນວປະຕິບັດທີ່ດີທີ່ສຸດຂອງ ລະຫັດທີ່ປອດໄພ. ນອກຈາກນັ້ນ ຊ່ວຍຫັນປ່ຽນແຮງງານໃນວົງກວ້າງ ຂຶ້ນໂດຍການອັບເດດການແນວປະຕິບັດໃນ ການຈ້າງງານເພື່ອປະເມີນ ຄວາມຮູ້ດ້ານຄວາມປອດໄພ ແລະ ເຮັດວຽກກັບມະຫາວິທະ ຍາໄລ ວິທະຍາໄລຊຸມຊົນ ບູດແຄ້ມ ແລະ ນັກການສຶກສາອື່ນໆເພື່ອເຊື່ອມ ປະສານການຮັກສາຄວາມປອດໄພເຂົ້າໃນຫຼັກສູດການພັດທະນາ ວິທະຍາສາດຄອມພິວເຕີ ແລະ ຊອັບແວ.

[3] NIST SSDF, PO 1.2, ຕົວຢ່າງ 2: "ກຳນົດນະໂຍບາຍທີ່ລະບຸຄວາມຕ້ອງການດ້ານຄວາມປອດໄພສຳລັບຊອັບແວຂອງອົງກອນ ແລະ ກວດສອບການປະຕິບັດຕາມຈຸດສຳຄັນໃນ SDLC (ເຊັ່ນ: ປະເພດຂອງຂໍ້ບົກພ່ອງຂອງຊອັບແວທີ່ກວດສອບໂດຍເກດ ການຕອບສະໜອງຕໍ່ຊ່ອງໂຫວ່ທີ່ຄົ້ນພົບໃນຊອັບແວທີ່ປ່ອຍອອກມາ)."

7. **ທົດສອບການຈັດການເຫດການດ້ານຄວາມປອດໄພ (SIEM) ແລະ ການປະສົມປະສານການຮັກສາຄວາມປອດໄພ ລະບົບອັດຕະໂນມັດ ແລະ ການຕອບສະໜອງ (SOAR).** ນອກເໜືອຈາກການດຳເນີນການທົດສອບພາກສະໜາມແລ້ວ ໃຫ້ເຮັດວຽກຮ່ວມກັນກັບຜູ້ໃຫ້ບໍລິການ SIEM ແລະ SOAR ທີ່ນິຍົມໂດຍສົມທົບກັບລູກຄ້າທີ່ໄດ້ຮັບເລືອກເພື່ອທຳຄວາມເຂົ້າໃຈວ່າທີມງານຕອບໂຕ້ເຫດການໃຊ້ບັນທຶກເພື່ອກວດສອບເຫດການທີ່ສົງໃສ ຫຼື ເຫດການດ້ານຄວາມປອດໄພຕົວຈິງໄດ້ແນວໃດ. ນັກພັດທະນາຊອບແວຈຳນວນນ້ອຍທີ່ມີປະສົບການໃນການຕອບສະໜອງຕໍ່ເຫດການໃດໜຶ່ງ ແລະ ອາດຈະສ້າງບັນທຶກທີ່ບໍ່ໄດ້ຊ່ວຍເຫຼືອຜູ້ປະເຊີນເຫດການຫຼາຍເທົ່າທີ່ພວກເຂົາຄາດຫວັງ. ດ້ວຍການເຮັດວຽກກັບທັງເທັກໂນໂລຢີ SIEM ແລະ SOAR ແລະ ຜູ້ຊ່ຽວຊານດ້ານການຕອບໂຕ້ຕໍ່ເຫດການທີ່ແທ້ຈິງ, ທີມງານພັດທະນາສາມາດສ້າງບັນທຶກທີ່ບອກເລົ່າເລື່ອງທີ່ຖືກຕ້ອງ ແລະ ຄົບຖ້ວນ ປະຫຍັດເວລາ ແລະ ຫຼຸດຜ່ອນຄວາມບໍ່ແນ່ນອນໃນເວລາເກີດເຫດ.

8. **ສອດຄ່ອງກັບ Zero Trust Architecture (ZTA).** ຈັດວາງຄຳແນະນຳການນຳໃຊ້ຜະລິດຕະພັນໃຫ້ສອດຄ່ອງກັບ ຕົວຢ່າງເຊັ່ນ ໂມເດລ NIST ZTA ແລະ CISA Zero Trust Maturity. ຊຸກຍູ້ໃຫ້ລູກຄ້ານຳຫຼັກການເຫຼົ່ານີ້ເຂົ້າໄປໃຊ້ໃນສະພາບແວດລ້ອມຂອງຕົນ.

ຫຼັກການທາງທຸລະກິດດ້ານຄວາມປອດໄພ

1. **ໃຫ້ການບັນທຶກໂດຍບໍ່ເສຍຄ່າເພີ່ມເຕີມ.** ການບໍລິການລະບົບຄລາວດ໌ຄວນມຸ່ງໝັ້ນທີ່ຈະສ້າງ ແລະ ເກັບຮັກສາບັນທຶກທີ່ກ່ຽວ ຂ້ອງກັບຄວາມປອດໄພໂດຍບໍ່ມີຄ່າໃຊ້ຈ່າຍເພີ່ມເຕີມ. ຜະລິດຕະພັນຢູ່ໃນອົງກອນກໍ່ຄວນສ້າງບັນທຶກທີ່ກ່ຽວຂ້ອງກັບຄວາມປອດໄພໂດຍບໍ່ມີຄ່າໃຊ້ຈ່າຍເພີ່ມເຕີມເຊັ່ນກັນ. ນອກຈາກນັ້ນ, ຜະລິດຕະພັນຄວນບັນທຶກເຫດການດ້ານຄວາມປອດໄພຕາມຄ່າເລີ່ມຕົ້ນເນື່ອງຈາກລູກຄ້າຫຼາຍຄົນອາດຈະບໍ່ເຂົ້າໃຈຄຸນຄ່າຂອງພວກເຂົາຈົນກວ່າຫຼັງຈາກຈະເກີດເຫດການຂຶ້ນ. ຍຸດທະວິທີເຫຼົ່ານີ້ອາດຈະຕ້ອງມີການທົບທວນຄືນຢ່າງລະອຽດກ່ຽວກັບເຫດການດ້ານຄວາມປອດໄພໃດທີ່ຄວນຈະຖືກບັນທຶກໄວ້ເພື່ອໃຫ້ຮັບຮູ້ເຖິງສະຖານະຄວາມປອດໄພທາງໄຊເບີ, ລູກຄ້າສາມາດຕັ້ງຄ່າການບັນທຶກແນວໃດ ເກັບຮັກສາບັນທຶກໃນໄລຍະເວລາໃດ, ການຮັກສາຄວາມຖືກຕ້ອງຂອງບັນທຶກ ແລະ ການເກັບຮັກສາ ແລະ ວິທີການວິເຄາະບັນທຶກ. ໃນບາງກໍລະນີ ການທົບທວນຄືນອາດຈະແນະນຳເຖິງຄວາມຈຳເປັນໃນການປັບໂຄງສ້າງຂອງການຈັດການບັນທຶກຂອງແອັບ ພລິເຄຊັນໃໝ່ ເພື່ອຊ່ວຍເຮັດໃຫ້ພວກເຂົາດຳເນີນການໄດ້ ແລະ ມີຄ່າໃຊ້ຈ່າຍທີ່ເໝາະສົມກັບຜູ້ຜະລິດ. ການເຮັດວຽກກັບຜູ້ຊ່ຽວຊານດ້ານການຕອບສະໜອງຕໍ່ເຫດການ (IR) ສາມາດເພີ່ມໂອກາດທີ່ບັນທຶກຈະເປັນປະໂຫຍດຕໍ່ຜູ້ສອບສວນໃນພາກສະໜາມ. ເບິ່ງພາກສ່ວນກ່ຽວກັບ SIEMs.

2. **ລົບລ້າງພາສີທີ່ເຊື່ອງໄວ້.** ເຜີຍແຜ່ຄຳໝັ້ນສັນຍາທີ່ຈະບໍ່ຄິດຄ່າບໍລິການດ້ານຄວາມປອດໄພ ຫຼື ຄວາມເປັນສ່ວນຕົວ ຫຼື ການລວມເຂົ້າກັນ. ຕົວຢ່າງ ພາຍໃນຂອບເຂດທີ່ໃຫຍ່ຂຶ້ນຂອງການຄຸ້ມຄອງຂໍ້ມູນປະຈຳຕົວ ແລະ ການເຂົ້າເຖິງ (IAM), ມີບໍລິການທີ່ເອີ້ນວ່າການບໍລິການລົງຊື່ພຽງຄັ້ງດຽວ (SSO). ຜູ້ຜະລິດບາງຄົນຈະຄິດຄ່າບໍລິການເພີ່ມເຕີມເພື່ອເຊື່ອມຕໍ່ລະບົບຂອງພວກເຂົາກັບການບໍລິການ SSO (ບາງຄັ້ງເອີ້ນວ່າຜູ້ໃຫ້ບໍລິການຂໍ້ມູນລະບຸຕົວຕົນ) "ພາສີ SSO" ນີ້ໝາຍຄວາມວ່າ ຂໍ້ມູນປະຈຳຕົວ ແລະ ການຄຸ້ມຄອງການເຂົ້າເຖິງທີ່ດີນັ້ນແມ່ນບໍ່ສາມາດເຂົ້າເຖິງ SMOs ຈຳນວນຫຼາຍ, ປ້ອງກັນບໍ່ໃຫ້ພວກເຂົາບັນລຸມາດຕາການຮັກສາຄວາມປອດໄພທີ່ເຂັ້ມແຂງ. ບາງບໍລິການຄິດຄ່າບໍລິການເພີ່ມເຕີມເພື່ອເປີດໃຊ້ MFA ສຳລັບຜູ້ໃຊ້. **ຄວາມປອດໄພບໍ່ຄວນຖືກຕັ້ງລາຄາເປັນຂອງຟຸ່ມເຟືອຍ ແຕ່ຖືວ່າເປັນສິດຂອງລູກຄ້າ.** ຜູ້ຜະລິດບາງຄົນໄດ້ໂຕ້ຖຽງວ່າມີລູກຄ້າຈຳນວນໜ້ອຍທີ່ຮ້ອງຂໍຄຸນສົມບັດເຫຼົ່ານີ້ ແລະ ເຂົາເຈົ້າມີຄ່າໃຊ້ຈ່າຍເພີ່ມເຕີມໃນການບຳລຸງຮັກສາ. ການໂຕ້ຖຽງເຫຼົ່ານີ້ບໍ່ສົນໃຈຕໍ່ຄວາມຈິງທີ່ວ່າມີລູກຄ້າຈຳນວນໜ້ອຍທີ່ຈະໂທມາຮ້ອງຮຽນ ຫຼື ຕໍ່ລອງ ບໍ່ແມ່ນລູກຄ້າທັງໝົດຈະເຂົ້າໃຈຢ່າງແທ້ຈິງວ່າຜົນປະໂຫຍດຂອງຄຸນສົມບັດເຫຼົ່ານີ້ມີປະໂຫຍດແນວໃດ ແລະ ຄຸນສົມບັດທັງໝົດມີຄ່າໃຊ້ຈ່າຍໃນການບຳລຸງຮັກສາ. ແຕ່ພວກເຮົາບໍ່ເຫັນຜູ້ຜະລິດຈຳນວນຫຼາຍຄິດຄ່າບໍລິການເພີ່ມເຕີມສຳລັບຄວາມພ້ອມໃຊ້ງານ ຫຼື ຄວາມສົມບູນຂອງຂໍ້ມູນ. ຄ່າໃຊ້ຈ່າຍໃນການສະໜັບສະໜູນ ຄຸນລັກສະນະທີ່ສຳຄັນເຫຼົ່ານັ້ນແມ່ນໄດ້ຮວມຢູ່ໃນລາຄາທີ່ລູກຄ້າທຸກຄົນຈ່າຍ ເຊັ່ນດຽວກັນກັບຄ່າໃຊ້ຈ່າຍໃນການລວມເອົາສາຍແອວນິລະໄພ ຄໍພວງມາໄລແບບເລື່ອນຂຶ້ນລົງໄດ້ ແລະ ຖົງລົມນິລະໄພທີ່ຊ່ວຍຊີວິດຜູ້ປະສົບອຸປະຕິເຫດ.

3. **ຍອມຮັບມາດຕະຖານແບບເປີດ.** ໃຊ້ມາດຕະຖານແບບເປີດ ໂດຍສະເພາະກ່ຽວກັບເຄືອຂ່າຍທົ່ວໄປ ແລະ ໂປຣໂຕຄອລການລະບຸຕົວຕົນ. ຫຼີກລ້ຽງໂປຣໂຕຄອລທີ່ເປັນກຳມະສິດເມື່ອມີມາດຕະຖານແບບເປີດ.

4. **ໃຫ້ເຄື່ອງມືອັບເກຣດ.** ລູກຄ້າຫຼາຍຄົນລັງເລທີ່ຈະຮັບເອົາຜະລິດຕະພັນລຸ້ນລ້າສຸດ ລວມທັງການນຳໃຊ້ຄຸນສົມບັດ ໃໝ່ ແລະ ປອດໄພກວ່າ ເຊັ່ນ ການເຊື່ອມຕໍ່ເຄືອຂ່າຍທີ່ປອດໄພ. ຜູ້ຜະລິດຊອບແວສາມາດເພີ່ມການຮັບຮອງເອົາການອັບເກຣດໃໝ່ຂອງລູກຄ້າໂດຍການຈັດຫາເຄື່ອງມືເພື່ອຊ່ວຍຫຼຸດຜ່ອນຄວາມບໍ່ແນ່ນອນ ແລະ ຄວາມສ່ຽງ. ສະເໜີໃບອະນຸຍາດຟຣີໃຫ້ກັບລູກຄ້າເພື່ອທົດສອບການອັບເກຣດ ແລະ ແພຊໃນສະພາບແວດລ້ອມການທົດສອບເພື່ອເປັນແນວທາງໃນການຈູງໃຈລູກຄ້າ.

ຫຼັກການ ທີ 2: ຮັບເອົາຄວາມໂປ່ງໃສ ແລະ ຄວາມຮັບຜິດຊອບຂັ້ນຮຸນແຮງ

ຄຳອະທິບາຍ

ຜູ້ຜະລິດຊອັບແວຄວນມີຄວາມພາກພູມໃຈໃນການນຳສະເໜີຜະລິດຕະພັນທີ່ປອດໄພ ແລະ ໝັ້ນຄົງ ຕະຫຼອດຈົນສ້າງຄວາມແຕກຕ່າງ ຈາກສ່ວນທີ່ເຫຼືອຂອງຊຸມຊົນຜູ້ຜະລິດລາຍອື່ນໆໂດຍອີງໃສ່ຄວາມສາມາດໃນການເຮັດຂອງຕົນ.

ພວກເຮົາມາແກ້ໄຂຄວາມກັງວົນທົ່ວໄປກ່ຽວກັບຄວາມໂປ່ງໃສກັນດີກວ່າ. ໃນເວລາທີ່ຜູ້ປະຕິບັດງານປຶກສາຫາລືກ່ຽວກັບຄວາມໂປ່ງໃສ ຂັ້ນຮຸນແຮງ, ການສົນທະນາກໍມີທ່າອ່ຽງທີ່ຈະຕິດຂັດດ້ວຍຄວາມກັງວົນວ່າພວກເຂົາກຳລັງຈັດຕຽມ "ແຜນງານສຳລັບຜູ້ໂຈມຕີ." ຢ່າງໃດກໍ່ຕາມ, ຫຼັກຖານທີ່ລົ້ນເຫຼືອແມ່ນວ່າຜູ້ໂຈມຕີກຳລັງດຳເນີນໄປໄດ້ດີຖ້າບໍ່ມີແຜນງານດັ່ງກ່າວ ແລະ ຄວາມກັງວົນດັ່ງກ່າວຄວນ ຄິດເຖິງຄວາມໂປ່ງໃສທີ່ໃຫ້ຜົນປະໂຫຍດແກ່ ລູກ ຄ້າໂດຍກົງ ລູກຄ້າໂດຍທາງອ້ອມ ຕ່ອງໂສ້ການສະໜອງ ແລະ ອຸດສາຫະກຳ ຊອັບແວ ທັງໝົດ.

ຄວາມໂປ່ງໃສຊ່ວຍໃຫ້ອຸດສາຫະກຳສ້າງຕັ້ງແບບແຜນ ຫຼື ອີກຄວາມໜຶ່ງວ່າ, ສິ່ງທີ່ "ດີ" ມີລັກສະນະແນວໃດ. ມັນຊ່ວຍໃຫ້ແບບແຜນ ເຫຼົ່ານັ້ນປ່ຽນແປງໄປຕາມການເວລາເພື່ອຕອບສະໜອງຄວາມຕ້ອງການຂອງລູກຄ້າ, ການປ່ຽນແປງກົນລະຍຸດຂອງນັກສະແດງ ໄພຂົ່ມຂູ່ ຫຼື ເສດຖະກິດ ຫຼື ວິວັດທະນາການຂອງເທັກໂນໂລຢີ. ຄວາມໂປ່ງໃສຊ່ວຍໃຫ້ຜູ້ຜະລິດທີ່ມີຊັບພະຍາກອນໜ້ອຍລົງຮຽນຮູ້ ຈາກຜູ້ທີ່ມີຊັບພະຍາ ກອນທີ່ໃຫຍ່ ແລະ ມີຄວາມສາມາດກວ່າ. ການສົນທະນາກ່ຽວກັບການແບ່ງປັນຂໍ້ມູນຄວນຂະຫຍາຍອອກໄປ ນອກເໜືອກວ່າຕົວຊີ້ບອກໄພຂົ່ມຂູ່ໃນເວລາຈິງ, ເພື່ອກວມອົງປະກອບຂ້າງລຸ່ມນີ້.

ຄວາມໂປ່ງໃສບັງຄັບໃຫ້ມີການຕັດສິນໃຈກ່ຽວກັບການຮັກສາຄວາມປອດໄພທີ່ຕ້ອງເຮັດໃນຕອນຕົ້ນໆຂອງຂະບວນການພັດທະນາ ແລະ ເປັນກິດຈະກຳຢ່າງຕໍ່ເນື່ອງຂອງຜູ້ນຳທຸລະກິດເຊັ່ນດຽວກັນກັບວິສະວະກອນ ແລະ ຜູ້ຊ່ຽວຊານດ້ານຄວາມປອດໄພ. ຄວາມໂປ່ງໃສ ສ້າງຄວາມຮັບຜິດຊອບໃນຜະລິດຕະພັນ.

ໝາຍເຫດກ່ຽວກັບທາງເລືອກຂອງ ຄຸນນາມ "radical" ຢູ່ທາງໜ້າຂອງ "transparency". ໃນທຸກມື້ນີ້ ມັນເປັນເລື່ອງແປກທີ່ຜູ້ຜະລິດຊອັບແວທີ່ຈະເຜີຍແຜ່ຂໍ້ມູນໂດຍລະອຽດກ່ຽວກັບວິທີການພັດທະນາ ແລະ ບຳລຸງຮັກສາຊອັບແວ ແລະ ວິທີທີ່ພວກເຂົາພັດທະນາໂປຣແກຣມຂອງພວກເຂົາໂດຍໃຊ້ຂໍ້ມູນໃນເວລາຜ່ານໄປ. ໃນອຸດສາຫະກຳຊອັບແວ, ຜູ້ຜະລິດຈຳນວນໜ້ອຍທີ່ສະເໜີການທ່ຽວຊົມວິທີການອອກແບບຊອັບແວຂອງຕົນ. ມີໂອກາດໜ້ອຍສຳລັບຜູ້ຜະລິດຊອັບແວທີ່ຈະໄດ້ເຫັນວ່າອົງກອນທີ່ຄ້າຍຄືກັນຈັດໂຄງສ້າງໂປຣແກຣມ SDLC ຂອງເຂົາແນວໃດ ແລະ ໂປຣແກຣມເຫຼົ່ານັ້ນຢູ່ໃນສະພາບແວດລ້ອມຂອງລູກຄ້າຕໍ່ກັບຜູ້ໂຈມຕີທີ່ແທ້ຈິງໄດ້ແນວໃດ. ອຸດສາຫະກຳລວມຈະໄດ້ຮັບຜົນປະໂຫຍດຈາກການແບ່ງປັນຂໍ້ມູນເພີ່ມເຕີມກ່ຽວກັບຫົວຂໍ້ຕ່າງໆເຊັ່ນ ກົນລະຍຸດໃນການວັດແທກຄ່າໃຊ້ຈ່າຍຂອງຄວາມບົກພ່ອງດ້ານຄວາມປອດໄພ ແລະ ການກຳຈັດປະເພດຂອງຊ່ອງໂຫວ່. ເປັນຜົນມາຈາກແນວປະຕິບັດທົ່ວໄປເຫຼົ່ານີ້ ຜູ້ຜະລິດຊອັບແວທຸກຄົນຕ້ອງຮຽນຮູ້ວິທີການຈັດການກັບຄວາມປອດໄພຂອງຜະລິດຕະພັນດ້ວຍຕົນເອງ. ບາງທີໂດຍການບໍ່ເກັບພາສີທີ່ຟຸ່ມເຟືອຍກ່ຽວກັບຄຸນສົມບັດດ້ານຄວາມປອດໄພ ດັ່ງນັ້ນຄວາມປອດໄພຈຶ່ງກາຍເປັນສູນຄ່າໃຊ້ຈ່າຍແທນທີ່ຈະເປັນສູນກຳໄລ ແລະ ບໍລິສັດຕ່າງໆກໍຈະໄດ້ຮັບຜົນປະໂຫຍດຈາກການແບ່ງເບົາພາລະຜ່ານການເຮັດວຽກຮ່ວມກັນ ແລະ ຄວາມໂປ່ງໃສ.

ພວກເຮົາຕ້ອງການທີ່ຈະສຸມໃສ່ກົນລະຍຸດທີ່ຈະເລັ່ງການວິວັດທະນາຂອງອຸດສາຫະກຳຊອັບແວ. ພວກເຮົາບໍ່ສາມາດທີ່ຈະສວຍໂອກາດ ແລະ ເຮັດການປັບປຸງເພີ່ມເຕີມໄດ້ອີກຕໍ່ໄປ. ຖ້າຫາກວ່າພວກເຮົາຈະເອົາຊະນະໄພຂົ່ມຂູ່ທີ່ເກີດຂຶ້ນຈາກສັດຕູທີ່ສະຫຼາດ ແລະ ການປັບຕົວຮ່ວມກັນ, ພວກເຮົາຕ້ອງຍອມຮັບເອົາລະດັບຄວາມໂປ່ງໃສທີ່ຈະຮູ້ສຶກບໍ່ສະບາຍໃຈໃນປັດຈຸບັນ ແຕ່ຈະຊ່ວຍຂັບເຄື່ອນອຸດສາຫະກຳກ້າວໄປຂ້າງໜ້າ. ໃນປັດຈຸບັນມີຜູ້ຜະລິດຜູ້ທີ່ລວບລວມເຫຼົ່ານີ້ບາງສ່ວນໄວ້ຢ່າງປອດໄພຕາມຫຼັກການການອອກແບບ. ດັ່ງທີ່ ວິລລຽມ ກິບສັນ ກ່າວໄວ້ "ອະນາຄົດມາເຖິງແລ້ວ, ພຽງແຕ່ມີການ ແຈກຢາຍບໍ່ເທົ່າທຽມກັນເທົ່ານັ້ນ." **ຄວາມໂປ່ງໃສຂັ້ນສູງສຸດຈະຊ່ວຍແຈກຢາຍຂໍ້ມູນນັ້ນ ແລະ ໃຫ້ຜົນປະໂຫຍດແກ່ຜູ້ປົກປ້ອງຫຼາຍກວ່າຝ່າຍກົງກັນຂ້າມຂອງພວກເຮົາ.**

ຄວາມໂປ່ງໃສສາມາດເຮັດໄດ້ຫຼາຍກວ່າການຊ່ວຍໃຫ້ອົງກອນລະດັບດຽວກັນພັດທະນາ SDLCs ຂອງພວກເຂົາເຕີບໃຫຍ່ໄດ້. ລູກຄ້າ ແລະ ນັກລົງທຶນໃນອະນາຄົດສາມາດຮຽນຮູ້ເພີ່ມເຕີມກ່ຽວກັບການລົງທຶນ ແລະ ການແລກປ່ຽນທີ່ຜູ້ຜະລິດໄດ້ເຮັດໄວ້ ແລະ ມາດຕາການການຮັກສາຄວາມປອດໄພທີ່ການລົງທຶນເຫຼົ່ານັ້ນໄດ້ສ້າງຂຶ້ນສຳລັບລູກຄ້າ. ຜູ້ຜະລິດທີ່ຍອມຮັບຄວາມໂປ່ງໃສຂັ້ນສຸງສຸດຈະໃຫ້ຂໍ້ມູນແກ່ລູກຄ້າເພື່ອຊ່ວຍພວກເຂົາໃນການຕັດສິນໃຈຊື້ ບໍ່ພຽງແຕ່ກ່ຽວກັບລາຄາ ແລະ ຄຸນສົມບັດເທົ່ານັ້ນ ແຕ່ຍັງກວມເຖິງຄວາມປອດໄພອີກນຳ.

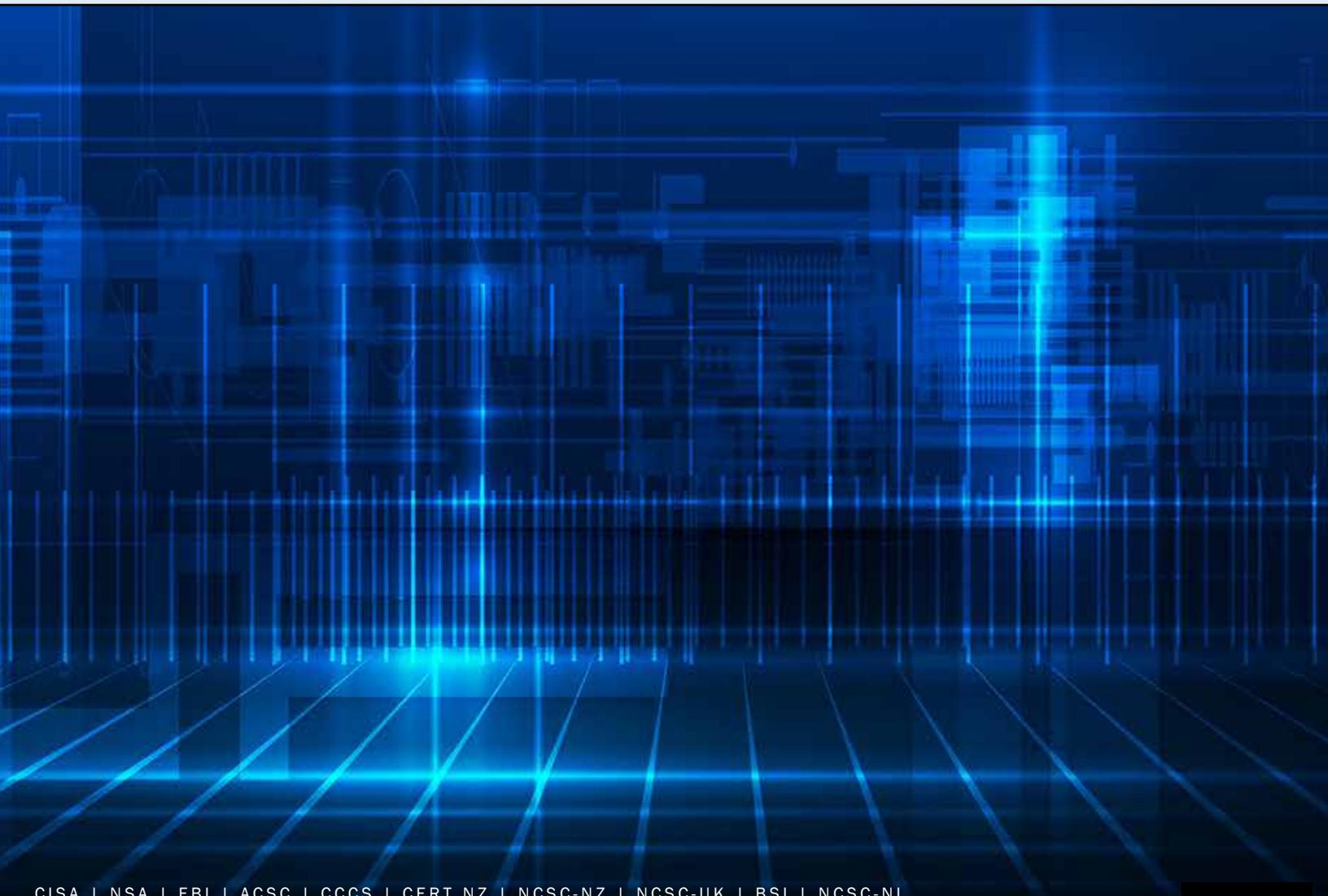
ເຖິງແມ່ນວ່າອົງກອນຈະເຮັດວຽກໜັກເພື່ອຮັກສາຄວາມປອດໄພລະບົບຕ່ອງໂສ້ການສະໜອງ ແລະ SDLC ຂອງພວກເຂົາ ກໍຕາມ ບໍລິສັດຕ່າງໆ ຕ່າງກໍປະສົບບັນຫາຂະບວນການສ້າງຂອງຕົນຖືກຫຼຸດໜ້ອຍ ລົງໃນອະດີດທີ່ຜ່ານມາ. ການຮັບເອົາຄວາມໂປ່ງໃສລະດັບສູງຄວນນຳໄປສູ່ການເປີດເຜີຍຕໍ່ສາທາລະນະກ່ຽວກັບການໂຈມຕີເຊັ່ນດຽວກັນກັບການປັບປຸງທີ່ບໍລິສັດໄດ້ເຮັດເພື່ອປ້ອງກັນ ແລະ ກວດພົບການໂຈມຕີໃນອະນາຄົດ. ຮູບແບບຂອງການແບ່ງປັນຂໍ້ມູນນັ້ນຈະຊ່ວຍໃຫ້ອົງກອນອື່ນໆຮຽນຮູ້ໂດຍບໍ່ຈຳເປັນຕ້ອງປະສົບກັບຊະຕາກຳດຽວກັນ.

ສາທິດຫຼັກການນີ້

ເພື່ອສາທິດຫຼັກການນີ້, ຜູ້ຜະລິດຊອັບແວຄວນດຳເນີນຕາມຂັ້ນຕອນຕ່າງໆລວມທັງດັ່ງຕໍ່ໄປນີ້:

ຫຼັກການຄວາມປອດໄພໂດຍຄ່າເລີ້ມຕົ້ນ

1. **ເຜີຍແຜ່ສະຖິຕິ ແລະ ແນວໂນ້ມທີ່ກ່ຽວຂ້ອງລວມດ້ານຄວາມປອດໄພ.** ຫົວຂໍ້ຕົວຢ່າງລວມມີການຮັບຮອງເອົາ MFA ມາໃຊ້ໂດຍລູກຄ້າ ແລະ ຜູ້ດູແລລະບົບ ແລະ ການໃຊ້ໂປຣໂຕຄອລເດີມທີ່ບໍ່ປອດໄພ.
2. **ເຜີຍແຜ່ສະຖິຕິ patching.** ໃຫ້ລາຍລະອຽດວ່າເປີເຊັນຂອງລູກຄ້າທີ່ໃຊ້ຜະລິດຕະພັນມີລຸ້ນຫຼ້າສຸດ ແລະ ສິ່ງທີ່ທ່ານກຳລັງເຮັດເພື່ອເຮັດໃຫ້ການອັບເດດງ່າຍຂຶ້ນ ແລະ ເຊື່ອຖືໄດ້ຫຼາຍຂຶ້ນ.
3. **ເຜີຍແຜ່ຂໍ້ມູນກ່ຽວກັບສິດທິພິເສດທີ່ບໍ່ໄດ້ໃຊ້.** ເຜີຍແຜ່ຂໍ້ມູນລວມກ່ຽວກັບການອະນຸຍາດທີ່ຫຼາຍເກີນໄປໃນທົ່ວຖານລູກຄ້າຂອງທ່ານຕະຫຼອດເຖິງການກະຕຸ້ນເຕືອນ ແລະ ການປ່ຽນແປງອື່ນໆຂອງຜະລິດຕະພັນທີ່ທ່ານກຳລັງເຮັດເພື່ອຫຼຸດຜ່ອນພື້ນທີ່ການໂຈມຕີຂອງລູກຄ້າ. ສິດທິພິເສດທີ່ບໍ່ໄດ້ໃຊ້ເຫຼົ່ານີ້ມີແນວໂນ້ມທີ່ຈະເປັນໂຕເລືອກທີ່ດີສຳລັບການແຈ້ງເຕືອນຜູ້ດູແລລະບົບ ເຊັ່ນ ສຽງເຕືອນໃສ່ສາຍເຂັມຂັດນິລະໄພ.



ຫຼັກການໃນການພັດທະນາຜະລິດຕະພັນທີ່ປອດໄພ

1. **ສ້າງການຄວບຄຸມຄວາມປອດໄພພາຍໃນ.** ຫຼາຍບໍລິສັດໄດ້ເຫັນຜົນປະໂຫຍດຂອງການເຄື່ອນຍ້າຍຂໍ້ມູນຂອງເຂົາເຈົ້າໄປຫາຜູ້ໃຫ້ບໍລິການລະບົບຄລາວດ໌. ດຽວນີ້ຜູ້ໃຫ້ບໍລິການຄລາວດ໌ເຫຼົ່ານັ້ນກາຍເປັນເປົ້າໝາຍຂອງຜູ້ໂຈມຕີ. ຜູ້ໃຫ້ບໍລິການຊອັບແວໃນຖານະບໍລິການ (SaaS)ຄວນເຜີຍແຜ່ສະຖິຕິຂອງການຄວບຄຸມພາຍໃນຂອງຕົນ. ຕົວຢ່າງ ຜູ້ໃຫ້ບໍລິການ SaaS ຄວນເຜີຍແຜ່ສະຖິຕິກ່ຽວກັບການນຳໃຊ້ພາຍໃນຂອງ MFA ທີ່ປ້ອງກັນການຟິຊຊິ່ງ,ພາຍໃນຂອງຕົນ ເຊັ່ນ ການພິສູດຢືນຢັນຕົວຕົນແບບ Fast Identity Online (FIDO). ເວົ້າໄດ້ວ່າບໍ່ມີພະນັກງານຄົນໃດສາມາດເຂົ້າເຖິງຂໍ້ມູນຂອງລູກຄ້າ ຫຼື ຂໍ້ມູນລະອຽດອ່ອນອື່ນໆ ໄດ້ໂດຍບໍ່ມີການພິສູດຢືນຢັນຜ່ານ MFA ທີ່ປ້ອງກັນການ ຟິຊຊິ່ງ.

2. **ເຜີຍແຜ່ຮູບແບບໄພຂົ່ມຂູ່ທີ່ຮຸນແຮງ** ຜະລິດຕະພັນຄວາມປອດໄພໂດຍການອອກແບບເລີ່ມຕົ້ນດ້ວຍຕົວແບບໄພຂົ່ມຂູ່ທີ່ເປັນລາຍລັກອັກສອນທີ່ອະທິບາຍເຖິງສິ່ງທີ່ຜູ້ສ້າງພະຍາຍາມປົກປ້ອງ ແລະ ຈາກໃຜ. ຮູບແບບໄພຂົ່ມຂູ່ທີ່ມີປະສິດຕິຜົນແມ່ນໄດ້ຖືກແຈ້ງໃຫ້ຮູ້ໂດຍວິທີການທີ່ບຸກລຸກເກີດຂຶ້ນ ແລະ ຄວນຈະກວມເອົາທັງວິສາຫະກິດ ແລະ ສະພາບແວດລ້ອມການພັດທະນາ ເຊັ່ນດຽວກັນກັບວິທີການທີ່ຜູ້ຜະລິດຊອັບແວຕັ້ງໃຈທີ່ຈະນຳໃຊ້ໃນສະພາບແວດລ້ອມຂອງລູກຄ້າ.

3. **ເຜີຍແຜ່ການຢັ້ງຢືນຕົນເອງ SDLC ທີ່ປອດໄພແບບລະອຽດ.** ຜູ້ຜະລິດທີ່ປະຕິບັດຕາມ NIST SSDF ຫຼື ກອບວຽກທີ່ຄ້າຍຄືກັນອື່ນໆກຳລັງເຮັດວຽກຢ່າງຫ້າວຫັນເພື່ອມຸ່ງໄປສູ່ວົງຈອນການພັດທະນາຊອັບແວທີ່ສົມບູນ. ການເຜີຍແຜ່ການຢືນຢັນຕົນເອງວ່າການຄວບຄຸມໃດທີ່ຜູ້ຜະລິດໄດ້ບັງຄັບໃຊ້ ແລະ ສຳລັບຜະລິດຕະພັນໃດ ຈະສະແດງໃຫ້ເຫັນຄວາມມຸ່ງໝັ້ນທີ່ຈະຍຶດໝັ້ນໃນການປະຕິບັດທີ່ດີທີ່ສຸດເຫຼົ່ານີ້ ແລະ ເພີ້ມລະດັບຄວາມໝັ້ນໃຈໃຫ້ແກ່ລູກຄ້າຂອງຕົນ ໂຄງການການຢືນຢັນອື່ນໆລວມມີ ວິທີການລະບົບຕ່ອງໂສ້ການສະໜອງ ຂອງ ອິສຣາແອລ ດ້ານໄຊເບີ(Israel Cyber Supply Chain Methodology) ເປັນຕົ້ນ.

4. **ຍອມຮັບຄວາມໂປ່ງໃສຂອງຊ່ອງໂຫວ່.** ເຜີຍແຜ່ຄວາມມຸ່ງໝັ້ນທີ່ຈະເຮັດໃຫ້ແນ່ໃຈວ່າຊ່ອງໂຫວ່ຂອງຜະລິດຕະພັນທີ່ລະບຸໄວ້ຈະຖືກເຜີຍແຜ່ເປັນລາຍການ CVE ທີ່ຖືກຕ້ອງ ແລະ ຄົບຖ້ວນ. ມັນເປັນຄວາມຈິງໂດຍສະເພາະສຳລັບພາກສະໜາມການຄົດໄລ່ຈຸດອ່ອນທົ່ວໄປທີ່ລະບຸສາເຫດທີ່ແທ້ຈິງຂອງຊ່ອງໂຫວ່. ຍິ່ງຖານຂໍ້ມູນ CVE ສາທາລະນະຖືກຕ້ອງ ແລະ ຄົບຖ້ວນຫຼາຍຂຶ້ນ ອຸດສາຫະກຳກໍຈະຍິ່ງສາມາດຕິດຕາມໄດ້ວ່າຜະລິດຕະພັນມີຄວາມປອດໄພຫຼາຍຂຶ້ນແນວໃດ ແລະ ປະເພດຊ່ອງໂຫວ່ໃດແດ່ທີ່ມີຫຼາຍທີ່ສຸດ. ຢ່າງໃດກໍ່ຕາມ ຈົ່ງລະວັງການລໍ້ລວງໃຫ້ນັບ CVEs ເປັນຕົວຊີ້ທາງລົບ ເພາະວ່າຕົວເລກດັ່ງກ່າວຍັງເປັນສັນຍານຂອງຊຸມຊົນການວິເຄາະ ແລະ ການທົດສອບລະຫັດທີ່ດີອີກດ້ວຍ. ໃນຂະນະທີ່ຜູ້ຜະລິດໃຊ້ປັດຊະຍາຄວາມປອດໄພໂດຍການອອກແບບ ເປັນໄປໄດ້ວ່າໃນຕອນທຳອິດຈຳນວນ CVE ດິບຂອງພວກເຂົາຈະເພີ່ມຂຶ້ນ ເນື່ອງຈາກການຄົ້ນພົບທີ່ສົມບູນແບບ ແລະ ການແກ້ໄຂຊ່ອງໄຫວ່ໃນລະຫັດທີ່ມີຢູ່. ຜູ້ຜະລິດຄວນເຜີຍແຜ່ການວິເຄາະກ່ຽວກັບຊ່ອງໂຫວ່ໃນອະດີດ ລວມເຖິງຮູບແບບ ແລະມາດຕະການຕ່າງໆທີ່ຖືກປະຕິບັດເພື່ອແກ້ໄຂບັນດາຊ່ອງໂຫວ່ທັງໝົດທຸກລະດັບ. ຕົວຢ່າງ, ຖ້າ CVEs ຂອງບໍລິສັດສ່ວນໃຫຍ່ກ່ຽວຂ້ອງກັບການຂຽນແບບຂ້າມໄຊທ໌ (XSS), ຈັດທຳເອກະສານການວິເຄາະສາເຫດອັນແທ້ຈິງ ການຕອບໂຕ້ (ເຊັ່ນ: ການປ່ຽນໄປສູ່ກອບແມ່ແບບເວັບທີ່ປ້ອງກັນ XSS), ແລະ ຜົນໄດ້ຮັບຈະເປັນສັນຍານໃຫ້ລູກຄ້າຮູ້ວ່າພວກເຂົາ ຈະບໍ່ຖືກຕົກເປັນເຫຍື່ອຂອງກຸ່ມຄວາມອ່ອນແອປະເພດໜຶ່ງທີ່ການຫຼຸດຜ່ອນຜົນກະທົບເປັນທີ່ເຂົ້າໃຈມາໃນຫຼາຍທົດສະວັດ.

5. **ເຜີຍແຜ່ ລາຍການ ວັດຖຸ ຊອັບແວ [Software Bills of Materials (SBOMs)].** ຜູ້ຜະລິດຄວນມີອຳນາດຄວບຄຸມຕ່ອງໂສ້ການສະໜອງຂອງພວກເຂົາ. ອົງກອນຄວນສ້າງ ແລະ ບຳລຸງຮັກສາ SBOMs [2] ສຳລັບແຕ່ລະຜະລິດຕະພັນ ຂໍຂໍ້ມູນຈາກຜູ້ສະໜອງຂອງພວກເຂົາ ແລະ ເຮັດໃຫ້ SBOMs ສາມາດໃຊ້ໄດ້ສຳລັບລູກຄ້າ ແລະ ຜູ້ໃຊ້ລົງຕາມກະແສ. ສິ່ງນີ້ຈະຊ່ວຍສະແດງໃຫ້ເຫັນເຖິງຄວາມດຸໝັ່ນຂອງພວກເຂົາໃນການທຳຄວາມເຂົ້າໃຈອົງປະກອບທີ່ພວກເຂົານຳໃຊ້ໃນການສ້າງຜະລິດຕະພັນ ຄວາມສາມາດໃນການຕອບສະໜອງຕໍ່ຄວາມສ່ຽງທີ່ໄດ້ລະບຸໃໝ່ ແລະ ສາມາດຊ່ວຍໃຫ້ລູກຄ້າເຂົ້າໃຈວິທີການຕອບສະໜອງຖ້າຫາກວ່າໜຶ່ງຂອງໂມດູນໃນລະບົບຕ່ອງໂສ້ການສະໜອງມີຊ່ອງໂຫວ່ທີ່ພົບເຫັນໃໝ່.

ເພື່ອເປັນຂໍ້ມູນອ້າງອີງ ກະຊວງເສດຖະກິດ ການຄ້າ ແລະອຸດສາຫະກຳ ຂອງຍີ່ປຸ່ນ (METI) ໄດ້ຈັດພິມເຜີຍແຜ່ "Guide of Introduction of Software Bill of Materials (SBOM) "ຄູ່ມືການແນະນຳຂອງ Software Bill of Materials (SBOM) ສຳລັບການຄຸ້ມຄອງຊອັບແວ." ຄວາມໂປ່ງໃສຄວນຂະຫຍາຍໄປສູ່ເຟີມແວໃນອຸປະກອນທີ່ຝັງຕົວ ແລະ ຂໍ້ມູນ ແລະ ແບບຈຳລອງທີ່ໃຊ້ໃນການຮຽນຮູ້ຂອງ AI/ມາຊີນ ເລີນນິ່ງ (ML). ນອກເໜືອໄປຈາກການຊ່ວຍເຫຼືອໃນການຕັດສິນໃຈຊື້ ແລະ ຄວາມສາມາດໃນການດຳເນີນງານແລ້ວ, SBOMs ຍັງມີບົດບາດສຳຄັນໃນໂຄງສ້າງພື້ນຖານໃນການກວດສອບ ແລະ ຕອບສະໜອງຕໍ່ການໂຈມຕີລະບົບຕ່ອງໂສ້ການສະໜອງທີ່ເປັນອັນຕະລາຍ ອີກນຳ.

6. **ເຜີຍແຜ່ນະໂຍບາຍການເປີດເຜີຍຊ່ອງໂຫວ່.** ເຜີຍແຜ່ນະໂຍບາຍການເປີດເຜີຍຊ່ອງໂຫວ່ທີ່ (1) ອະນຸຍາດການທົດສອບກັບຜະລິດຕະພັນທັງໝົດທີ່ນຳສະເໜີໃຫ້ໂດຍຜູ້ຜະລິດ ແລະ ເງື່ອນໄຂສຳລັບການທົດສອບເຫຼົ່ານັ້ນ, (2) ໃຫ້ຄວາມຄຸ້ມຄອງທາງກົດໝາຍສຳລັບການປະຕິບັດທີ່ສອດຄ່ອງກັບນະໂຍບາຍ ແລະ (3) ອະນຸຍາດໃຫ້ເປີດເຜີຍຕໍ່ສາທາລະນະ ຊ່ອງໂຫວ່ຫຼັງຈາກລະຍະ ເວລາທີ່ກຳນົດໄວ້. ຜູ້ຜະລິດຄວນທຳການວິເຄາະຕົ້ນເຫດຂອງຊ່ອງໂຫວ່ທີ່ຄົ້ນພົບ ແລະ ດຳເນີນການເພື່ອກຳຈັດກຸ່ມຊ່ອງໂຫວ່ທັງໝົດມາໄດ້ຫຼາຍທີ່ສຸດ. ເບິ່ງ ແມ່ແບບນະໂຍບາຍການເປີດເຜີຍຊ່ອງໂຫວ່ ຂອງ CISA ສຳລັບພາສາອ້າງອີງ.

ຫຼັກການທາງທຸລະກິດດ້ານຄວາມປອດໄພລະດັບມືອາຊີບ

1. **ເປີດເຜີຍຊື່ທີ່ປອດໄພໂດຍຜູ້ສະໜັບສະໜູນຜູ້ບໍລິຫານລະດັບສູງດ້ານການອອກແບບ.** ໃນຫຼາຍອົງກອນ ການຮັກສາຄວາມປອດໄພ (ເຊັ່ນ ຄຸນນະພາບ) ໄດ້ຖືກມອບໝາຍໃຫ້ທີມງານດ້ານວິຊາການທີ່ມີຄວາມສາມາດໃນການປ່ຽນແປງໂຄງສ້າງເພື່ອປັບປຸງຄວາມປອດໄພຂອງຜະລິດຕະພັນຢ່າງຫຼວງຫຼາຍ ການຕັ້ງຊື່ຜູ້ບໍລິຫານທຸລະກິດລະດັບລະສູງຕໍ່ສາທາລະນະເພື່ອດູແລໂປຣແກຣມຄວາມປອດໄພໂດຍການອອກແບບຈະປ່ຽນຄວາມປອດໄພຂອງຜະລິດຕະພັນໄປສູ່ຄວາມກັງວົນກ່ຽວກັບທຸລະກິດລະດັບສູງສຸດ.

2. **ເຜີຍແຜ່ແຜນງານຄວາມປອດໄພໂດຍການອອກແບບ.** ຜູ້ຜະລິດຄວນບັນທຶກການປ່ຽນແປງທີ່ເຮັດກັບ SDLC ຂອງຕົນເພື່ອປັບປຸງຄວາມປອດໄພຂອງລູກຄ້າ ລວມທັງລາຍລະອຽດກ່ຽວກັບບົດລາຍງານການທົດສອບພາກສະໜາມ ການດຳເນີນການເພື່ອກຳຈັດຊ່ອງໂຫວ່ປະເພດຕ່າງໆທັງໝົດ ແລະ ລາຍການອື່ນໆທີ່ລະບຸໄວ້ໃນຫຼັກການອື່ນໆ. ເຊັ່ນດຽວກັບໃນກໍລະນີຂອງຄວາມພະຍາຍາມໃນການປັບປຸງຄຸນນະພາບ ໂປຣແກຣມການປັບປຸງຄວາມປອດໄພມີໄລຍະທີ່ມີຂັ້ນຕອນ ການວາງແຜນ ການຄວບຄຸມ ແລະ ການປັບປຸງທີ່ແຕກຕ່າງກັນ. ດ້ວຍຈິດວິນຍານຂອງການສະແດງໃຫ້ເຫັນແທນທີ່ຈະເປັນການບອກ, ເຜີຍແຜ່ແຜນງານ ແລະ ລາຍລະອຽດທີ່ຢູ່ເບື້ອງຫຼັງຂອງໄລຍະເຫຼົ່ານີ້ຈະສ້າງຄວາມໝັ້ນໃຈວ່າຜະລິດຕະພັນມີຄວາມປອດໄພໂດຍການອອກແບບ. ຫຼັງຈາກບັນລຸຄວາມກ້າວໜ້າທີ່ສຳຄັນແລ້ວ ຜູ້ຜະລິດສາມາດໃຫ້ລາຍລະອຽດໃຫ້ໃນບົດລາຍງານຄວາມໂປ່ງໃສໄດ້. ການເຮັດດັ່ງນັ້ນບໍ່ພຽງແຕ່ສະແດງໃຫ້ເຫັນຄວາມມຸ່ງໝັ້ນຕໍ່ແນວປະຕິບັດຄວາມປອດໄພໂດຍການອອກແບບເທົ່ານັ້ນ ແຕ່ຍັງສາມາດເປັນແຮງບັນດານໃຈຄົນອື່ນໃຫ້ນຳໃຊ້ໂປຣແກຣມທີ່ຄ້າຍຄືກັນໂດຍສະແດງໃຫ້ເຫັນຫຼັກຖານທີ່ມີຢູ່ແລ້ວ.

3. **ເຜີຍແຜ່ແຜນງານດ້ານຄວາມປອດໄພຂອງໜ່ວຍຄວາມຈຳ.** ຜູ້ຜະລິດສາມາດດຳເນີນການເພື່ອກຳຈັດໃນກຸ່ມຊ່ອງໂຫວ່ທີ່ໃຫຍ່ທີ່ສຸດກຸ່ມໜຶ່ງໂດຍການຍ້າຍຜະລິດຕະພັນທີ່ມີຢູ່ແລ້ວ ແລະ ສ້າງຜະລິດຕະພັນໃໝ່ໂດຍໃຊ້ພາສາທີ່ປອດໄພຂອງໜ່ວຍຄວາມຈຳ. ໃນຂະນະທີ່ການດຳເນີນການນີ້ອາດຈະບໍ່ເປັນໄປໄດ້ໃນທຸກກໍລະນີ ແຕ່ຜູ້ຜະລິດສາມາດພິຈາລະນາພັດທະນາ ແອັບພລິເຄຊັນແຮັບເປີ (Application Wrapper) ໃນພາສາທີ່ປອດໄພຂອງໜ່ວຍຄວາມຈຳແທນທີ່ຈະຂຽນແອັບພລິເຄຊັ່ນທັງໝົດຄືນໃໝ່. ນອກຈາກນີ້ຍັງອາດລວມເຖິງວິທີທີ່ຜູ້ຜະລິດກຳລັງອັບເດດການຈ້າງງານ ການຝຶກອົບຮົມ ການກວດສອບລະຫັດ ແລະ ຂະບວນການພາຍໃນອື່ນໆ ຕະຫຼອດຈົນວິທີການທີ່ພວກເຂົາກຳລັງຊ່ວຍໃຫ້ຊຸມຊົນ ໂອເພັນຊອຣ໌ສ ເຮັດເຊັ່ນດຽວກັນ.

4. **ເຜີຍແຜ່ຜົນໄດ້ຮັບ.** ໃນຂະນະທີ່ອັບເດດ SDLC ເພື່ອລວບລວມປັດຊະຍາຄວາມປອດໄພໂດຍການອອກແບບ, ອົງກອນຈະພົບກັບໄຊຊະນະຢ່າງໄວ ໄຊຊະນະທີ່ເຂັ້ມງວດທາງດ້ານຊັບພະຍາກອນຫຼາຍຂຶ້ນ ແລະ ບາງຂໍ້ເສັຍທີ່ບໍ່ຄາດຄິດ. ໂດຍການນຳສະເໜີຄວາມສຳເລັດພາຍໃນ ແລະ ອຸປະສັກຕ່າງໆ ທົ່ວທັງອຸດສາຫະກຳສາມາດຮຽນຮູ້ຈາກຜົນໄດ້ຮັບ.

ຫຼັກການທີ 3: ນຳຈາກທາງເທິງ

ຄຳອະທິບາຍ

ເຖິງແມ່ນວ່າປັດຊະຍາໂດຍລວມແມ່ນເອີ້ນວ່າ "ຄວາມປອດໄພໂດຍການອອກແບບ" ແຕ່ສິ່ງຈູງໃຈສຳລັບຄວາມປອດໄພຂອງລູກຄ້າເລີ່ມຕົ້ນກ່ອນຂັ້ນຕອນການອອກແບບຜະລິດຕະພັນ. ເລີ່ມຕົ້ນດ້ວຍເປົ້າໝາຍ ແລະ ຈຸດປະສົງທາງທຸລະກິດທີ່ແຝງຢູ່ ແລະ ຈະແຈ້ງ ແລະ ຜົນໄດ້ຮັບທີ່ຕ້ອງການ. ສະເພາະຜູ້ນຳລະດັບສູງເຮັດໃຫ້ຄວາມສຳຄັນກັບຄວາມປອດໄພເປັນບູລິມະສິດທາງທຸລະກິດ ການສ້າງແຮງຈູງໃຈພາຍໃນ ແລະສົ່ງເສີມວັດທະນະທຳແບບທົ່ວເຖິງເພື່ອເຮັດໃຫ້ການຮັກສາຄວາມປອດໄພເປັນຂໍ້ກຳນົດໃນການອອກແບບເທົ່ານັ້ນ ພວກເຂົາຈຶ່ງຈະບັນລຸຜົນໄດ້ຮັບທີ່ດີທີ່ສຸດ.

ໃນຂະນະທີ່ຄວາມຊ່ຽວຊານດ້ານເທັກນິກມີຄວາມສຳຄັນຕໍ່ຄວາມປອດໄພຂອງຜະລິດຕະພັນ ແຕ່ກໍບໍ່ແມ່ນເລື້ອງທີ່ຈະສາມາດປ່ອຍໃຫ້ເປັນໜ້າທີ່ຂອງເຈົ້າໜ້າທີ່ ດ້ານເທັກນິກພຽງຜູ້ດຽວ. ມັນເປັນລຳດັບຄວາມສຳຄັນທາງທຸລະກິດທີ່ຕ້ອງເລີ່ມຕົ້ນຈາກດ້ານເທິງສຸດ.

ບາງຄົນສົງໄສວ່າຜູ້ຜະລິດຊອັບແວກຳລັງຍອມຮັບຫຼັກການສອງຂໍ້ທຳອິດ ແລະ ສ້າງສິ່ງປະດິດທີ່ມີຄວາມໝາຍ ຫຼື ບໍ່ ຫຼັກການທີສາມຈຳເປັນ ຫຼື ບໍ? ວິທີທີ່ບໍລິສັດສ້າງວິໄສທັດ, ພາລະກິດ, ຄຸນຄ່າ ແລະ ວັດທະນະທຳທີ່ຈະສົ່ງຜົນຕໍ່ຜະລິດຕະພັນ ແລະ ອົງປະກອບເຫຼົ່ານັ້ນມີສ່ວນປະກອບທີ່ໜັກແໜ້ນຢູ່ທີ່ດ້ານເທິງສຸດ. ພວກເຮົາເຫັນສິ່ງນີ້ຢູ່ໃນອຸດສາຫະກຳອື່ນໆທີ່ມີການປັບປຸງດ້ານຄວາມປອດໄພ ແລະ ຄຸນນະພາບຢ່າງຫຼວງຫຼາຍ. ຜູ້ຊ່ຽວຊານດ້ານຄຸນນະພາບ J.M. Juran ຂຽນວ່າ:

> ***ການບັນລຸການເປັນຜູ້ນຳທີ່ມີຄຸນນະພາບຕ້ອງການໃຫ້ຜູ້ຈັດການລະດັບສູງເປັນຜູ້ຮັບຜິດຊອບໃນການຄຸ້ມຄອງດ້ານຄຸນນະພາບດ້ວຍຕົນເອງ. ໃນບໍລິສັດທີ່ບັນລຸຄວາມເປັນຜູ້ນຳທີ່ມີຄຸນນະພາບ ຜູ້ຈັດການລະດັບສູງຈະເປັນຜູ້ຊີ້ນຳການລິເລີ່ມດັ່ງກ່າວເປັນສ່ວນຕົວ. ຂ້າພະເຈົ້າບໍ່ຮູ້ຂໍ້ຍົກເວັ້ນໃດໆ. [3]***

ພວກເຮົາເຊື່ອວ່າຄວາມປອດໄພເປັນໝວດໝູ່ຍ່ອຍຂອງຄຸນນະພາບຜະລິດຕະພັນ. ເມື່ອຄວາມປອດໄພ ແລະ ຄຸນນະພາບກາຍເປັນສິ່ງຈຳເປັນທາງທຸລະກິດ ແທນທີ່ຈະປ່ອຍໜ້າທີ່ທາງດ້ານເທັກນິກເຫຼືອໄວ້ສຳລັບເຈົ້າໜ້າທີ່ດ້ານເທັກນິກເທົ່ານັ້ນ, ອົງກອນຕ່າງໆຈະສາມາດຕອບສະໜອງຄວາມຕ້ອງການດ້ານຄວາມປອດໄພຂອງລູກຄ້າໄດ້ໄວ ແລະ ມີປະສິດທິພາບຫຼາຍຂຶ້ນ. ຍິ່ງໄປກວ່ານັ້ນ, ການລົງທຶນຊັບພະຍາກອນທີ່ຈຳເປັນເພື່ອຮັບປະກັນວ່າຄວາມປອດໄພຂອງຊອັບແວເປັນລຳດັບຄວາມສຳຄັນທາງທຸລະກິດຕັ້ງແຕ່ເລີ່ມຕົ້ນຈະຊ່ວຍຫຼຸດຜ່ອນຕົ້ນທຶນໃນໄລຍະຍາວໃນການແກ້ໄຂຂໍ້ບົກພ່ອງຂອງຊອັບແວ - ແລະ ໃນທາງກັບກັນ, ຫຼຸດຜ່ອນຄວາມສ່ຽງດ້ານຄວາມປອດໄພຂອງຊາດ.

ເຊັ່ນດຽວກັບທີ່ທີມຜູ້ນຳໄດ້ດຳ ເນີນໂຄງການຄວາມຮັບຜິດຊອບຕໍ່ສັງຄົມຂອງອົງກອນ (CSR), ກໍມີຄວາມຮັບຮູ້ເພີ່ມຫຼາຍຂຶ້ນວ່າຄະນະກຳມະການຂອງອົງກອນ ລວມທັງຜູ້ຜະລິດຊອັບແວ ຄວນມີບົດບາດຢ່າງຫ້າວຫັນໃນການຊີ້ນຳໂຄງການຮັກສາຄວາມປອດໄພທາງໄຊເບີ. ຄຳວ່າຄວາມຮັບຜິດຊອບທາງໄຊເບີຂອງອົງກອນ (CCR) ແມ່ນບາງຄັ້ງຖືກໃຊ້ເພື່ອອະທິບາຍຄວາມຄິດທີ່ເກີດຂຶ້ນໃໝ່ນີ້.

ສາທິດຫຼັກການນີ້

ເພື່ອສາທິດຫຼັກການນີ້ ຜູ້ຜະລິດຊອັບແວຄວນດຳເນີນຂັ້ນຕອນຕ່າງໆລວມທັງ ດັ່ງຕໍ່ໄປນີ້:

1. **ລວມເອົາລາຍລະອຽດຂອງໂປຣແກຣມຄວາມປອດໄພໂດຍການອອກແບບ ໄວ້ຢູ່ໃນບົດລາຍງານທາງດ້ານການເງິນຂອງອົງກອນ.** ຖ້າຜູ້ຜະລິດເປັນບໍລິສັດທີ່ມີການຊື້ຂາຍໃນສາທາລະນະ ໃຫ້ເພີ່ມພາກສ່ວນຢູ່ໃນແຕ່ລະບົດລາຍງານປະຈຳປີ ແຕ່ລະສະບັບທີ່ກ່ຽວຂ້ອງກັບຄວາມພະຍາຍາມໃນຄວາມປອດໄພໂດຍການອອກແບບ. ເປັນເລື່ອງປົກກະຕິທີ່ບົດລາຍງານທາງການເງິນປະຈຳປີຂອງລົດໃຫຍ່ທີ່ຈະປະກອບມີພາກສ່ວນກ່ຽວກັບຄວາມປອດໄພຂອງຜູ້ຂັບຂີ່ ແລະ ຜູ້ໂດຍສານ ລວມທັງຂໍ້ມູນກ່ຽວກັບຄະນະກຳມະການດ້ານຄຸນນະພາບ ແລະ ຄວາມປອດໄພແບບລວມສູນ ແລະ ແບບກະຈາຍ. ການໃຫ້ລາຍລະອຽດກ່ຽວກັບໂປແກຣມຄວາມປອດໄພໂດຍການອອກແບບໃນບົດລາຍງານທາງດ້ານການເງິນຈະສະແດງໃຫ້ເຫັນວ່າອົງກອນກຳລັງເຊື່ອມຕໍ່ຄວາມປອດໄພຂອງລູກຄ້າກັບຜົນໄດ້ຮັບທາງດ້ານການເງິນຂອງອົງກອນ ແລະ ບໍ່ພຽງແຕ່ນຳໃຊ້ຄຳສັບໃນເອກະສານການຕະຫຼາດມາໃຊ້ເທົ່ານັ້ນເນື່ອງຈາກເປັນສິ່ງທີ່ກຳລັງນິຍົມ.

2. **ສະໜອງບົດລາຍງານໃຫ້ຄະນະກຳມະການບໍລິຫານຂອງທ່ານຢ່າງສະໝ່ຳສະເໝີ.** ຫົວໜ້າເຈົ້າໜ້າທີ່ຮັກສາຄວາມປອດໄພຂໍ້ມູນຂ່າວສາ (CISO) ລາຍງານຕໍ່ຄະນະກຳມະການບໍລິຫານຂອງບໍລິສັດ ໂດຍປົກກະຕິແລ້ວ ຈະມີຂໍ້ມູນກ່ຽວກັບໂປຣແກຣມຄວາມປອດໄພໃນປະຈຸບັນ ແລະ ທີ່ວາງແຜນໄວ້ ໄພຂົ່ມຂູ່ ເຫດການດ້ານຄວາມປອດໄພທີ່ສົງໄສ ແລະ ໄດ້ຮັບການຢືນຢັນ ແລະ ການອັບເດດອື່ນໆທີ່ເນັ້ນໃສ່ມາດຕາການຄວາມປອດໄພ ແລະ ສຸຂະພາບຂອງບໍລິສັດ. ນອກເໜືອຈາກການໄດ້ຮັບຂໍ້ມູນກ່ຽວກັບມາດຕະການຄວາມປອດໄພຂອງອົງກອນແລ້ວ ຄະນະກຳມະການຄວນຂໍຂໍ້ມູນກ່ຽວກັບຄວາມປອດໄພຂອງຜະລິດຕະພັນ ແລະ ຜົນກະທົບຕໍ່ຄວາມປອດໄພຂອງລູກຄ້າ. ຄະນະກຳມະການບໍ່ຄວນເບິ່ງໄປທີ່ CISO ພຽງຢ່າງດຽວ, ແຕ່ຄວນເບິ່ງໄປທີ່ສະມາຊິກຄົນອື່ນໆ ຂອງຝ່າຍບໍລິຫານຂອງບໍລິສັດເປັນຫຼັກເພື່ອຫຼຸດຜ່ອນຄວາມສ່ຽງລູກຄ້າ.

3. **ສ້າງຄວາມເຂັ້ມແຂງໃຫ້ຜູ້ບໍລິຫານຄວາມປອດໄພໂດຍການອອກແບບ** ມີຄວາມແຕກຕ່າງກັນຢ່າງຫຼວງຫຼາຍລະຫວ່າງອົງກອນທີ່ທີມງານເທັກນິກມີ ່ການຍອມຮັບຈາກຜູ້ບໍລິຫານ,ຳ ແລະ ທີມທີ່ຜູ້ນຳທຸລະກິດຈັດການຂະບວນການປັບປຸງຄວາມປອດໄພຂອງລູກຄ້າເປັນການສ່ວນຕົວໂດຍໃຊ້ຂະບວນການທາງທຸລະກິດມາດຕະຖານ. ຄຳວ່າ ່ການຍອມຮັບຈາກຜູ້ບໍລິຫານ ຳ ໝາຍຄວາມວ່າຜູ້ໃດຜູ້ໜຶ່ງຕ້ອງຂາຍແນວຄວາມ ຄິດຂອງໂຄງການຄວາມປອດໄພຂອງລູກຄ້າແທນທີ່ຈະເປັນເປົ້າໝາຍທາງທຸລະກິດລະດັບສູງສຸດ. ຜູ້ບໍລິຫານນີ້ຕ້ອງໄດ້ຮັບອຳນາດທີ່ຈະມີອິດທິພົນຕໍ່ການລົງທຶນຂອງຜະລິດຕະພັນເພື່ອບັນລຸຜົນດ້ານຄວາມປອດໄພຂອງລູກຄ້າ.

4. **ສ້າງແຮງຈູງໃຈພາຍໃນທີ່ມີຄວາມໝາຍ.** ໃນຂະນະທີ່ມີສະຕິທີ່ຈະບໍ່ສ້າງແຮງຈູງໃຈທີ່ບິດເບືອນໄປທາງຜິດ ແຕ່ໃຫ້ວາງລະບົບການໃຫ້ລາງວັນເພື່ອປັບປຸງຄວາມປອດໄພຂອງລູກຄ້າໃຫ້ກົງກັບພຶດຕິກຳ ແລະ ຜົນໄດ້ຮັບທີ່ມີຄຸນຄ່າອື່ນໆ. ຈາກຄວາມປອດໄພໂດຍການອອກແບບໂດຍປູ້ບໍລິຫານໄປຈົນເຖິງການຄຸ້ມຄອງຜະລິດຕະພັນ ການພັດທະນາຊອັບແວ ການສະໜັບສະໜູນ ການຂາຍ,ທາງດ້ານກົດໝາຍ ແລະ ອົງກອນອື່ນໆ, ສາມຕໍ່ ແຮງຈູງໃຈດ້ານຄວາມປອດໄພຂອງລູກຄ້າເຂົ້າໄປໃນການຈ້າງງານ ການເລື່ອນຕຳແໜ່ງ ເງິນເດືອນ ໂບນັດ ທາງເລືອກຫຼັກຊັບ ແລະ ຂະບວນການທົ່ວໄປອື່ນໆໃນການດຳເນີນງານຂອງທຸລະກິດ. ຕົວຢ່າງ ເມື່ອສ້າງເງື່ອນໄຂສຳລັບການສົ່ງເສີມນັກພັດທະນາຊອັບແວ ໃຫ້ລວມຂໍ້ຄວນພິຈາລະນາການປັບປຸງຄວາມປອດໄພຂອງຜະລິດຕະພັນພ້ອມກັບມາດຕະຖານອື່ນໆເຊັ່ນ ເວລາອອນລາຍ, ປະສິດທິພາບ ແລະການປັບປຸງຄຸນນະສົມບັດ.

5. **ສ້າງສະພາຄວາມປອດໄພໂດຍການອອກແບບ.** ໃນບາງອຸດສາຫະກຳ ເປັນເລື່ອງປົກກະຕິສຳລັບອົງກອນຕ່າງໆ ທີ່ຈະສ້າງສະພາຄຸນນະພາບສ່ວນກາງ ແລະ ຝັງຕົວແທນດ້ານຄຸນນະພາບຢູ່ໃນພະແນກການສຳຄັນ ຫຼື ໜ່ວຍງານທຸລະກິດ. ໂດຍການລວມທັງສະມາຊິກແບບລວມສູນ ແລະ ແບບກະຈາຍ, ກຸ່ມເຫຼົ່ານີ້ເຮັດວຽກເພື່ອປັບປຸງຄຸນນະພາບຕໍ່ກັບເປົ້າໝາຍລະດັບສູງສຸດໃນຂະນະທີ່ໄດ້ຮັບ ການກວດວັດແທກທາງໄກຈາກສ່ວນເລິກໃນອົງກອນ. ເຊັ່ນດຽວກັນ, ສະພາຄວາມປອດໄພໂດຍການອອກແບບຈະປັບປຸງຄວາມປອດໄພຕໍ່ກັບເປົ້າໝາຍຂອງຄວາມປອດໄພໂດຍການອອກແບບໃນທົ່ວອົງກອນ.

6. **ສ້າງ ແລະ ພັດທະນາສະພາລູກຄ້າ.** ຜູ້ຜະລິດຊອັບແວຈຳນວນຫຼາຍມີສະພາລູກຄ້າທີ່ປະກອບດ້ວຍລູກຄ້າຈາກພາກພື້ນ, ອຸດສາຫະກຳ ແລະ ຂະໜາດຕ່າງໆ. ສະພາເຫຼົ່ານີ້ສາມາດສະໜອງຂໍ້ມູນຈຳນວນຫຼວງຫຼາຍກ່ຽວກັບຄວາມສຳເລັດຂອງລູກຄ້າ ແລະ ສິ່ງທ້າທາຍໃນການນຳໃຊ້ຜະລິດຕະພັນຂອງບໍລິສັດ. ຈັດໂຄງສ້າງວາລະການປະຊຸມສະພາດ້ວຍຫົວຂໍ້ສະເພາະເພື່ອແກ້ໄຂບັນຫາຄວາມປອດໄພຂອງລູກຄ້າ ເຖິງແມ່ນວ່າຜູ້ເຂົ້າຮ່ວມຈະບໍ່ຄິດວ່າເປັນຈຸດເດັ່ນກໍຕາມ. ພິຈາລະນາວ່າສະພາລູກຄ້າລາຍງານບ່ອນໃດ ແລະ ວິທີເຂົ້າເຖິງຜູ້ເຂົ້າຮ່ວມເພື່ອຄວາມເຂົ້າໃຈກ່ຽວກັບຄວາມປອດໄພຂອງຜະລິດຕະພັນຕາມທີ່ວາງໄວ້. ຕົວຢ່າງ ສະພາມີອະຄະຕິຕໍ່ຈຸດປະສົງການຕະຫຼາດ ແລະ ການຂາຍ ຫຼື ການຄຸ້ມຄອງຜະລິດຕະພັນບໍ? ຄວາມປອດໄພໂດຍຜູ້ບໍລິຫານດ້ານການອອກແບບຄວນຊ່ວຍຊີ້ນຳການໂຕ້ຕອບລູກຄ້າ ເຫຼົ່ານີ້ ແລະ ຄວນເຊື່ອມໂຍງກັບອົງປະກອບອື່ນໆໃນເອກະສານນີ້, ເຊັ່ນ ການສຶກສາພາກສະໜາມ.

ຄວາມປອດໄພໂດຍຍຸດທະວິທີການອອກແບບ

ຂອບການພັດທະນາຊອັບແວທີ່ປອດໄພ (SSDF), ຫຼື ເອີ້ນກັນວ່າ ສະຖາບັນມາດຕະຖານ ແລະ ເຕັກໂນໂລຊີແຫ່ງຊາດ (NIST's) SP 800-218, ແມ່ນຊຸດຫຼັກຂອງການພັດທະນາຊອັບແວທີ່ປອດໄພລະດັບສູງ ແນວປະຕິບັດທີ່ສາມາດປະສົມປະສານເຂົ້າກັບໃນແຕ່ລະຂັ້ນຕອນຂອງວົງຈອນການພັດທະນາຊອັບແວ (SDLC). ການປະຕິບັດຕາມການປະຕິບັດເຫຼົ່ານີ້ສາມາດຊ່ວຍໃຫ້ຜູ້ຜະລິດຊອັບແວມີປະສິດຕິພາບຫຼາຍຂຶ້ນໃນການຄົ້ນຫາ ແລະ ກຳຈັດຊ່ອງໂຫວ່ໃນຊອັບແວທີ່ປ່ອຍອອກມາ, ຫຼຸດຜ່ອນຜົນກະທົບທີ່ອາດເກີດຂຶ້ນຈາກການສະແຫວງຫາຜົນປະໂຫຍດຈາກຊ່ອງໂຫວ່ ແລະ ແກ້ໄຂສາເຫດທີ່ແທ້ຈິງຂອງຊ່ອງໂຫວ່ເພື່ອປ້ອງກັນການເກີດຊ້ຳອີກໃນອະນາຄົດ.

ອົງກອນຜູ້ຂຽນສົ່ງເສີມການນຳໃຊ້ຄວາມປອດໄພໂດຍຍຸດທະວິທີການອອກແບບ ລວມທັງຫຼັກການທີ່ອ້າງອີງເຖິງແນວປະຕິບັດ ຂອງ SSDF. ຜູ້ຜະລິດຊອັບແວຄວນພັດທະນາແຜນງານທີ່ເປັນລາຍລັກອັກສອນເພື່ອຮັບຮອງເອົາຄວາມປອດໄພຫຼາຍຂຶ້ນໂດຍການອອກແບບແນວປະຕິບັດໃນການພັດທະນາຊອັບແວໃນທົ່ວຫຼັກຖານຂອງຄວາມສາມາດຂອງຕົນ ຕໍ່ໄປນີ້ແມ່ນບັນຊີລາຍການແນວປະຕິບັດທີ່ດີທີ່ສຸດໂດຍສະຫຼຸບແບບສັງເຂບ:

- **ພາສາການຂຽນໂປຣແກຣມທີ່ປອດໄພສຳລັບໜ່ວຍຄວາມຈຳ (SSDF PW.6.1).** ຈັດລຳດັບຄວາມສຳຄັນໃນການນຳໃຊ້ພາສາທີ່ປອດໄພຂອງໜ່ວຍຄວາມຈຳທຸກຄັ້ງທີ່ເປັນ ໄປໄດ້. ອົງກອນຜູ້ຂຽນຮັບຮູ້ວ່າການຫຼຸດຜ່ອນບັນຫາສະເພາະໜ່ວຍຄວາມຈຳອາດຈະເປັນປະໂຫຍດໃນຍຸດທະວິທີໄລຍະສັ້ນສຳລັບພື້ນຖານລະຫັດເກົ່າ. ຕົວຢ່າງລວມມີການປັບປຸງພາສາ C/C++, ການຫຼຸດຜ່ອນຮາດແວການຈັດວາງທີ່ຢູ່ແບບສຸ່ມ (ASLR), ຄວາມສົມບູນແບບການຄວບຄຸມ (CFI), ແລະ fuzzing. ເຖິງຢ່າງໃດກໍ່ຕາມ ມີຄວາມເຫັນດີເຫັນພ້ອມທີ່ເພີ່ມຂຶ້ນວ່າການຮັບຮອງເອົາພາສາການຂຽນໂປຣແກຣມທີ່ປອດໄພສຳລັບໜ່ວຍຄວາມຈຳສາມາດກຳຈັດຄວາມບົກຜ່ອງປະເພດນີ້ໄດ້ ແລະ ຜູ້ຜະລິດຊອັບແວຄວນຄົ້ນຫາວິທີການຮັບຮອງເອົາການໃຊ້ພາສາດັ່ງກ່າວ. ບາງຕົວຢ່າງຂອງພາສາທີ່ປອດໄພສຳລັບໜ່ວຍຄວາມຈຳທີ່ທັນສະໄໝ ລວມມີ C#, Rust, Ruby, Java, Go, ແລະ Swift. ອ່ານຂໍ້ມູນເພີ້ມເຕີມກ່ຽວກັບຄວາມປອດໄພຂອງໜ່ວຍຄວາມຈຳຂອງ NSA ເອກະສານຂໍ້ມູນ ສຳລັບຂໍ້ມູນເພີ່ມເຕີມ.

- **ຮາກຖານຄວາມປອດໄພຂອງຮາດແວ** ລວມເອົາຄຸນສົມບັດທາງສະຖາປັດຕະຍະກຳທີ່ເປີດໃຊ້ການປົກປ້ອງໜ່ວຍຄວາມຈຳແບບລະອຽດ, ເຊັ່ນທີ່ອະທິບາຍໄວ້ໂດຍ Capability Hardware Enhanced RISC Instructions ທີ່ສາມາດປັບປຸງປະສິດທິພາບຮາດແວ(CHERI) ຊຶ່ງສາມາດຂະຫຍາຍສະຖາປັດຕະຍະກຳ ຊຸດຄຳສັ່ງ Instruction-Set Architectures (ISAs) ຂອງຮາດແວແບບເດີມ, ເຊັ່ນດຽວກັນກັບຄຸນສົມບັດອື່ນໆເຊັ່ນ ໂມດູນເວທີທີ່ເຊື່ອຖືໄດ້ ແລະ ໂມດູນຄວາມປອດໄພຂອງຮາດແວ. ເພື່ອເບິ່ງຂໍ້ມູນເພີ່ມເຕີມ ຈົ່ງໄປທີ່ ໜ້າເວັບ CHERI ຂອງມະຫາວິທະຍາໄລ ແຄມບຣິດຈ໌.

- **ອົງປະກອບຊອັບແວທີ່ປອໄພ (SSDF PW 4.1).** ໄດ້ຮັບ ແລະ ບຳລຸງຮັກສາອົງປະກອບຊອັບແວທີ່ມີຄວາມປອດໄພດີ (ເຊັ່ນ ໄລແບຣຣີ ຊອັບແວ, ໂມດູນ, ສິ່ງກາງ, ກອບວຽກ) ຈາກຜູ້ພັດທະນາທາງການຄ້າ, ແຫຼ່ງເປີດໂອເພິນຊອຣ໌ສ ແລະ ພາກສ່ວນທີສາມອື່ນໆທີ່ຜ່ານການຢັ້ງຢືນເພື່ອໃຫ້ໝັ້ນໃຈໃນຄວາມປອດໄພທີ່ເຂັ້ມແຂງໃນຜະລິດຕະພັນຊອັບແວຜູ້ບໍລິໂພກ.

- **ກອບວຽກແມ່ແບບເວັບ (SSDF PW.5.1).** ໃຊ້ກອບແມ່ແບບເວັບທີ່ປະຕິບັດການຫຼົບລ່ຽງການປ້ອນຂໍ້ມູນຂອງຜູ້ໃຊ້ໂດຍອັດຕະໂນມັດເພື່ອຫຼີກເວັ້ນການໂຈມຕີເວັບເຊັ່ນ ການສະຄຣິບຂ້າມເວັບໄຊຕ໌.

- **ການສອບຖາມແບບພາຣາມິເຕີ (SSDF PW.5.1).** ໃຊ້ການສອບຖາມແບບພາລາມິເຕີແທນທີ່ຈະລວມເອົາການປ້ອນຂໍ້ມູນຂອງຜູ້ໃຊ້ໃນການສອບຖາມ ເພື່ອຫຼີກເວັ້ນການໂຈມຕີແບບແຊກ SQL.

- **ການທົດສອບຄວາມປອດໄພຂອງແອັບພລິເຄຊັນແບບຄົງທີ່ ແລະ ແບບເຄື່ອນໄຫວ (SAST/DAST)** (SSDF PW.7.2, PW.8.2). ໃຊ້ເຄື່ອງມືເຫຼົ່ານີ້ເພື່ອວິເຄາະແຫຼ່ງລະຫັດຂອງຜະລິດຕະພັນ ແລະ ພຶດຕິກຳຂອງແອັບພລິເຄຊັນເພື່ອກວດສອບແນວປະຕິບັດທີ່ທີ່ມີຄວາມສ່ຽງຕໍ່ຂໍ້ຜິດພາດ. ເຄື່ອງມືເຫຼົ່ານີ້ກວມເອົາບັນຫາຕ່າງໆຕັ້ງແຕ່ການຈັດການໜ່ວຍຄວາມຈຳທີ່ບໍ່ເໝາະສົມໄປຈົນເຖິງການສ້າງແບບສອບຖາມຖານຂໍ້ມູນທີ່ມີແນວໂນ້ມເກີດຂໍ້ຜິດພາດ (ເຊັ່ນ ການປ້ອນຂໍ້ມູນຂອງຜູ້ໃຊ້ທີ່ບໍ່ໄດ້ຮັບການແກ້ໄຂທີ່ນຳໄປສູ່ການແຊກ SQL). ເຄື່ອງມື SAST ແລະ DAST ສາມາດຖືກລວມເຂົ້າໃນຂະບວນການພັດທະນາ ແລະ ດຳເນີນການໂດຍອັດຕະໂນມັດໂດຍເປັນສ່ວນໜຶ່ງຂອງການພັດທະນາຊອັບແວ. SAST ແລະ DAST ຄວນເສີມການທົດສອບປະເພດອື່ນໆ, ເຊັ່ນ ການທົດສອບໜ່ວຍງານ ແລະ ການທົດສອບການປະສົມປະສານ ເພື່ອໃຫ້ແນ່ໃຈວ່າຜະລິດຕະພັນປະຕິບັດຕາມຂໍ້ກຳນົດດ້ານຄວາມປອດໄພທີ່ຄາດຫວັງໄວ້. ເມື່ອບັນຫາຖືກລະບຸ, ຜູ້ຜະລິດຄວນທຳການວິເຄາະສາເຫດທີ່ແທ້ຈິງເພື່ອແກ້ໄຂຊ່ອງໂຫວ່ຢ່າງເປັນລະບົບ.

- **ການກວດສອບລະຫັດ** (SSDF PW.7.1, PW.7.2). ພະຍາຍາມກວດສອບໃຫ້ແນ່ໃຈວ່າລະຫັດທີ່ສົ່ງເຂົ້າໄປໃນຜະລິດຕະພັນຜ່ານເຕັກນິກການຄວບຄຸມຄຸນນະພາບ ເຊັ່ນ ການທົບທວນແບບເພື່ອນມິດໂດຍຜູ້ພັດທະນາອື່ນໆ ຫຼື "ການສ້າງຄວາມຜິດພາດ."
- **ລາຍການ ວັດຖຸຊອັບແວ - Software Bill of Materials (SBOM)** (SSDF PS.3.2, PW.4.1). ລວມເອົາການສ້າງ SBOM[4] ເພື່ອໃຫ້ເບິ່ງເຫັນເຂົ້າໄປໃນຊຸດຂອງຊອັບແວທີ່ເຂົ້າໄປໃນຜະລິດຕະພັນ.
- **ໂປຣແກຣມເປີດເຜີຍຊ່ອງໂຫວ່** (SSDF RV.1.3). ສ້າງໂປຣແກຣມການເປີດເຜີຍຊ່ອງໂຫວ່ທີ່ຊ່ວຍໃຫ້ນັກວິໄຈດ້ານຄວາມປອດໄພລາຍງານຊ່ອງໂຫວ່ ແລະ ໄດ້ຮັບຄວາມຄຸ້ມຄອງທາງດ້ານກົດໝາຍໃນການເຮັດເຊັ່ນນັ້ນ. ເປັນສ່ວນໜຶ່ງຂອງການນີ້, ຜູ້ສະໜອງຄວນສ້າງຂະບວນການເພື່ອກຳນົດສາເຫດທີ່ແທ້ຈິງຂອງຊ່ອງໂຫວ່ທີ່ຄົ້ນພົບ. ຂະບວນການດັ່ງກ່າວຄວນລວມເຖິງການກຳນົດວ່າການຮັບຮອງເອົາແນວປະຕິບັດດ້ານຄວາມປອດໄພໂດຍການອອກແບບໃດໜຶ່ງໃນເອກະສານນີ້ (ຫຼື ການປະຕິບັດອື່ນໆທີ່ຄ້າຍຄືກັນ) ມາໃຊ້ຈະເປັນການຂັດຂວາງການເກີດຂອງຊ່ອງໂຫວ່ໄດ້ ຫຼື ບໍ່.
- **ຄວາມສົມບູນ ຂອງ CVE.** ກວດສອບໃຫ້ແນ່ໃຈວ່າ CVEs ທີ່ຖືກເຜີຍແຜ່ລວມມີສາເຫດທີ່ແທ້ຈິງ ຫຼື ການຄິດໄລ່ຈຸດອ່ອນທົ່ວໄປ (CWE) ເພື່ອເຮັດໃຫ້ການວິເຄາະກ່ຽວກັບຂໍ້ບົກພ່ອງຂອງການອອກແບບຄວາມປອດໄພຂອງຊອັບແວທົ່ວອຸດສາຫະກຳ. ເຖິງແມ່ນວ່າການກວດສອບໃຫ້ແນ່ໃຈວ່າທຸກໆ CVE ແມ່ນຖືກຕ້ອງ ແລະ ຄົບຖ້ວນອາດໃຊ້ເວລາເພີ້ມເຕີມ, ແຕ່ມັນຊ່ວຍໃຫ້ໜ່ວຍງານທີ່ແຕກຕ່າງກັນສາມາດສັງເກດເຫັນແນວໂນ້ມຂອງອຸດສາຫະກຳທີ່ມີປະໂຫຍດຕໍ່ຜູ້ຜະລິດ ແລະ ລູກຄ້າທັງໝົດ. ສຳລັບຂໍ້ມູນເພີ່ມເຕີມກ່ຽວກັບການຈັດການຊ່ອງໂຫວ່ ຈົ່ງເບິ່ງຄຳແນະນຳ ການຈັດປະເພດຊ່ອງໂຫວ່ສະເພາະຂອງຜູ້ມີສ່ວນຮ່ວມ ຂອງ Stakeholder-Stakeholder-Specific Vulnerability Categorization (SSVC).
- **ການປ້ອງກັນໃນທາງເລິກ.** ການອອກແບບໂຄງສ້າງພື້ນຖານເພື່ອໃຫ້ການປະນີປະນອມຂອງການຄວບຄຸມຄວາມປອດໄພຢ່າງດຽວບໍ່ໄດ້ເຮັດໃຫ້ເກີດການປະນີປະນອມຂອງລະບົບທັງໝົດ. ຕົວຢ່າງ ການກວດສອບໃຫ້ແນ່ໃຈວ່າສິດທິຂອງຜູ້ໃຊ້ແມ່ນຖືກຈັດໃຫ້ຢ່າງຈຳກັດ ແລະ ໃຊ້ລາຍການຄວບຄຸມການເຂົ້າເຖິງສາມາດຫຼຸດຜ່ອນຜົນກະທົບຂອງບັນຊີທີ່ຖືກບຸກລຸກໄດ້. ນອກຈາກນີ້, ເຕັກນິກແຊນບອັກຊິ່ງ (sandboxing) ຊອັບແວຍັງສາມາດກັກກັນຊ່ອງໂຫວ່ເພື່ອຈຳກັດການປະນີປະນອມຂອງແອັບພລິເຄຊັນທັງໝົດ.
- **ຕອບສະໜອງເປົ້າໝາຍປະສິດທິພາບຄວາມປອດໄພທາງໄຊເບີ (CPGs).** ອອກແບບຜະລິດຕະພັນທີ່ຕອບສະໜອງຕາມແນວປະຕິບັດດ້ານຄວາມປອດໄພຂັ້ນພື້ນຖານ. ເປົ້າໝາຍປະສິດທິພາບດ້ານຄວາມປອດໄພທາງໄຊເບີ ຂອງ CISA ອະທິບາຍມາດຕະການພື້ນຖານດ້ານຄວາມປອດໄພທາງໄຊເບີທີ່ອົງກອນຕ່າງໆຄວນນຳໄປປະຕິບັດ. ນອກຈາກນັ້ນ ສຳລັບວິທີເພີ່ມເຕີມອື່ນໆເພື່ອເສີມສ້າງທ່າທາງຂອງອົງກອນຂອງທ່ານ, ຈົ່ງເບິ່ງ ການປະເມີນທາງໄຊເບີຂອງສະຫະຣາດຊະອານາຈັກ ກອບການເຮັດວຽກ ທີ່ມີຄວາມຄ້າຍຄືກັນກັບ CPGs ຂອງ CISA. ຖ້າຜູ້ຜະລິດບໍ່ສາມາດປະຕິບັດຕາມ CPGs - ເຊັ່ນວ່າບໍ່ຕ້ອງໃຊ້ MFA ທີ່ປ້ອງກັນການ ຟິຊຊິ່ງ ສຳລັບພະນັກງານທຸກຄົນ - ຫຼັງຈາກນັ້ນ, ກໍ່ຈະບໍ່ຖືວ່າຜະລິດຕະພັນດັ່ງກ່າວເປັນການຈັດສົ່ງ ຢ່າງປອດໄພດ້ວຍຜະລິດຕະພັນທີ່ມີການອອກແບບ.

ອົງກອນຜູ້ຂຽນຮັບຮູ້ວ່າການປ່ຽນແປງເຫຼົ່ານີ້ແມ່ນການປ່ຽນແປງທີ່ສຳຄັນໃນຈຸດຢືນຂອງອົງກອນ. ດັ່ງນັ້ນ, ການແນະນຳຂອງພວກເຂົາຈຶ່ງຄວນຈະຖືກຈັດລຳດັບຄວາມສຳຄັນໂດຍອີງໃສ່ການສ້າງແບບຈຳລອງໄພຂົ່ມຂູ່ທີ່ປັບແຕ່ງໂດຍສະເພາະ, ພາວະວິກິດ, ຄວາມຊັບຊ້ອນ ແລະ ຜົນກະທົບທາງທຸລະກິດ. ແນວປະຕິບັດເຫຼົ່ານີ້ສາມາດຖືກນຳໃຊ້ກັບຊອັບແວໃໝ່ ແລະ ຂະຫຍາຍເພີ່ມຂຶ້ນເພື່ອໃຫ້ກວມເອົາກໍລະນີການນຳໃຊ້ ແລະ ຜະລິດຕະພັນເພີ່ມເຕີມ. ໃນບາງກໍລະນີ ຄວາມວິກິດ ແລະ ລະດັບຄວາມສ່ຽງຂອງຜະລິດຕະພັນໃດໜຶ່ງອາດຈະເໝາະສົມກັບຕາຕະລາງການເລັ່ງເພື່ອຮັບຮອງເອົາແນວປະຕິບັດເຫຼົ່ານີ້ໄປໃຊ້. ໃນສ່ວນອື່ນໆ ແນວປະຕິບັດສາມາດຖືກນຳໄປໃສ່ໃນຖານລະຫັດແບບເດີມ ແລະ ແກ້ໄຂໄດ້ໃນເມື່ອເວລາຜ່ານໄປ.

[4] ບາງອົງກອນຜູ້ຂຽນກຳລັງຊອກຫາວິທີທາງອື່ນໃນການໄດ້ຮັບການຮັບຮອງດ້ານຄວາມປອດໄພໃນທົ່ວຕ່ອງໂສ້ການສະໜອງຊອັບແວ.

ยุดທະວິທີການຮັກສາຄວາມປອດໄພໂດຍຄ່າເລີ່ມຕົ້ນ

ນອກເໜືອຈາກການຮັບຮອງເອົາແນວປະຕິບັດໃນການພັດທະນາການອອກແບບມາໃຊ້ແລ້ວ ອົງກອນຜູ້ຂຽນຍັງແນະນຳໃຫ້ຜູ້ຜະລິດຊອັບແວ ຈັດລຳດັບຄວາມສຳຄັນຂອງການຮັກສາຄວາມປອດໄພໂດຍການກຳນົດ ຄ່າເລີ່ມຕົ້ນໃນຜະລິດຕະພັນຂອງຕົນ ສິ່ງເຫຼົ່ານີ້ຄວນພະຍາຍາມອັບເດດຜະລິດຕະພັນເພື່ອໃຫ້ສອດຄ່ອງກັບການປະຕິບັດເຫຼົ່ານີ້ຍ້ອນວ່າພວກເຂົາໄດ້ຮັບການປັບປຸງໃໝ່. ຍົກຕົວຢ່າງ:

- **ລົບລ້າງລະຫັດຜ່ານເລີ່ມຕົ້ນ.** ຜະລິດຕະພັນບໍ່ຄວນມາພ້ອມກັບລະຫັດຜ່ານເລີ່ມຕົ້ນທີ່ແບ່ງປັນກັນທົ່ວໄປ. ເພື່ອລົບລ້າງລະຫັດຜ່ານເລີ່ມຕົ້ນ, ອົງກອນຜູ້ຂຽນແນະນຳໃຫ້ຜະລິດຕະພັນກຳນົດໃຫ້ຜູ້ດູແລລະບົບຕັ້ງລະຫັດຜ່ານທີ່ຮັດກຸມໃນລະຫວ່າງການຕິດຕັ້ງ ແລະ ການຕັ້ງຄ່າ ຫຼື ເພື່ອໃຫ້ຜະລິດຕະພັນທີ່ຈະຈັດສົ່ງດ້ວຍລະຫັດຜ່ານທີ່ຮັດກຸມ ແລະ ເປັນເອກະລັກສຳລັບອຸປະກອນແຕ່ລະເຄື່ອງ.

- **ກຳນົດການກວດສອບສິດແບບຫຼາຍປັດໃຈ (MFA) ສຳລັບຜູ້ໃຊ້ທີ່ໄດ້ຮັບສິດທິພິເສດ.** ພວກເຮົາສັງເກດເຫັນວ່າ ວິສາຫະກິດຈຳນວນຫຼາຍແມ່ນຖືກຈັດການໂດຍຜູ້ດູແລລະບົບທີ່ບໍ່ໄດ້ປົກປ້ອງບັນຊີຂອງເຂົາເຈົ້າດ້ວຍ MFA. ເນື່ອງຈາກຜູ້ດູແລລະບົບແມ່ນເປົ້າໝາຍທີ່ມີມູນຄ່າສູງ, ຜະລິດຕະພັນຈຶງຄວນເລືອກບໍ່ຮັບ MFA ແທນທີ່ຈະເລືອກຮັບ. ນອກຈາກນັ້ນ ລະບົບຄວນແຈ້ງໃຫ້ຜູ້ດູແລລະບົບລົງທະບຽນຢູ່ໃນ MFA ເປັນປະຈຳຈົນກ່ວາພວກເຂົາຈະໄດ້ເປີດໃຊ້ງານ ຢູ່ໃນບັນຊີຂອງຕົນໄດ້ ຢ່າງສຳເລັດຜົນ. NCSC ຂອງເນເທີແລນດ໌ ມີຂໍ້ແນະນຳທີ່ຄ້າຍຄືກັບ CISA, ໃຫ້ເຂົ້າໄປເບິ່ງ ເອກະສານການພິສູດຢືນຢັນສະບັບສົມບູນ ສຳລັບຂໍ້ມູນເພີ່ມເຕີມ.

- **ການລົງຊື່ເຂົ້າສູ່ລະບົບຄັ້ງດຽວ (SSO).** ແອັບພລິເຄຊັ່ນດ້ານໄອທີຄວນປະຕິບັດການລົງຊື່ຄັ້ງດຽວຜ່ານມາດຕະຖານເປີດທີ່ທັນສະໄໝ. ຕົວຢ່າງເຊັ່ນ Security Assertion Markup Language (SAML) ຫຼື OpenID Connect (OIDC.) ຄວາມສາມາດນີ້ຄວນຈະພ້ອມໃຊ້ງານເປັນ ຄ່າເລີ່ມຕົ້ນໂດຍບໍ່ມີຄ່າໃຊ້ຈ່າຍເພີ່ມເຕີມ.

- **ບັນທຶກທີ່ປອດໄພ.** ໃຫ້ບັນທຶກການກວດສອບຄຸນນະພາບສູງແກ່ລູກຄ້າໂດຍບໍ່ເສຍຄ່າໃຊ້ຈ່າຍເພີ່ມເຕີມ ຫຼື ການຕັ້ງຄ່າເພີ່ມເຕີມ. ບັນທຶກການກວດສອບແມ່ນສຳຄັນສຳລັບການກວດສອບ ແລະ ເພີ້ມເຫດການດ້ານຄວາມປອດໄພທີ່ອາດເກີດຂຶ້ນ. ນອກຈາກນີ້ຍັງມີຄວາມສຳຄັນໃນລະຫວ່າງການສືບສວນກ່ຽວກັບເຫດການດ້ານຄວາມປອດໄພທີ່ໜ້າສົງໃສ ຫຼື ທີ່ໄດ້ຮັບການຢືນຢັນອີກດ້ວຍ. ພິຈາລະນາແນວປະຕິບັດທີ່ດີທີ່ສຸດເຊັ່ນການສະໜອງການເຊື່ອມໂຍງກັບຂໍ້ມູນຄວາມປອດໄພ ແລະ ລະບົບການຈັດການເຫດການ ທີ່ມີການໂຕ້ຕອບການຂຽນໂປຣແກຣມແອັບພລິເຄຊັ່ນ (API) ທີ່ໃຊ້ການປະສານງານເວລາສາກົນ (UTC), ການຈັດຮູບແບບໂຊນເວລາມາດຕະຖານ ແລະ ເຕັກນິກການຈັດທຳເອກະສານທີ່ມີປະສິດທິພາບ.

- **ໂປຣໄຟລ໌ການອະນຸຍາດຊອັບແວ.** ຜູ້ສະໜອງຊອັບແວຄວນໃຫ້ຄຳແນະນຳກ່ຽວກັບບົດບາດຂອງໂປຣໄຟລ໌ທີ່ໄດ້ຮັບອະນຸຍາດ ແລະ ກໍລະນີການນຳໃຊ້ທີ່ກຳນົດໄວ້. ຜູ້ຜະລິດຄວນມີຄຳເຕືອນທີ່ເຫັນໄດ້ຊັດເຈນເພື່ອແຈ້ງໃຫ້ລູກຄ້າຮູ້ເຖິງຄວາມສ່ຽງທີ່ເພີ່ມຂຶ້ນຖ້າພວກເຂົາບ່ຽງເບນຈາກການອະນຸຍາດໂປຼໄຟລ໌ທີ່ແນະນຳ. ຕົວຢ່າງ ທ່ານໝໍທາງການແພດສາມາດເບິ່ງບັນທຶກຂອງຄົນເຈັບທັງໝົດໄດ້ ແຕ່ຜູ້ຈັດກຳນົດການທາງການແພດມີຂໍ້ຈຳກັດໃນການເຂົ້າເຖິງຂໍ້ມູນບາງຢ່າງທີ່ຈຳເປັນສຳລັບການກຳນົດເວລາການນັດໝາຍ.

- **ຄວາມປອດໄພແບບເບິ່ງໄປຂ້າງໜ້າຫຼາຍກວ່າຄວາມເຂົ້າກັນໄດ້ແບບ ຍ້ອນກັບຫຼັງ.** ເລື້ອຍໆຄັ້ງທີ່ຄຸນສົມບັດດັ້ງເດີມທີ່ເຂົ້າກັນໄດ້ແບບຍ້ອນກັບຫຼັງແມ່ນຖືກລວມໄວ້ ແລະ ເປີດໃຊ້ງານເລື້ອຍໆ ໃນຜະລິດຕະພັນເຖິງວ່າຈະມີຄວາມສ່ຽງຕໍ່ຄວາມປອດໄພຂອງຜະລິດຕະພັນກໍຕາມ. ລຳດັບຄວາມສຳຄັນຂອງຄວາມປອດໄພຫຼາຍກວ່າຄວາມເຂົ້າກັນໄດ້ແບບຍ້ອນຫຼັງ ການສ້າງຄວາມເຂັ້ມແຂງໃຫ້ທີມງານຮັກສາຄວາມປອດໄພເພື່ອເອົາຄຸນສົມບັດທີ່ບໍ່ປອດໄພອອກເຖິງແມ່ນວ່າຈະເຮັດໃຫ້ເກີດການປ່ຽນແປງທີ່ຜິດພາດກໍຕາມ.

- **ຕິດຕາມ ແລະ ຫຼຸດຂະໜາດ ารຄູ່ມືການແຂງຕົວ.** ຫຼຸດຜ່ອນຂະໜາດຂອງ "ຄູ່ມືການແຂງຕົວ" ທີ່ລວມຢູ່ໃນຜະລິດຕະພັນ ແລະ ພະຍາຍາມຮັບປະກັນວ່າຂະໜາດຈະຫຼຸດລົງໃນເມື່ອເວລາຜ່ານໄປຍ້ອນວ່າຊອັບແວຮຸ່ນໃໝ່ຖືກປ່ອຍອອກມາ. ລວມອົງປະກອບຂອງ "ຄູ່ມືການແຂງຕົວ" ເປັນການຕັ້ງຄ່າເລີ່ມຕົ້ນຂອງຜະລິດຕະພັນ. ບັນດາອົງກອນຜູ້ຂຽນ ຮັບຮູ້ວ່າຄຳແນະນຳການແຂງຕົວສັ້ນລົງນັ້ນແມ່ນມາຈາກການຮ່ວມມືຢ່າງຕໍ່ເນື່ອງກັບລູກຄ້າທີ່ມີຢູ່ແລ້ວ ແລະ ລວມທັງຄວາມພະຍາຍາມຂອງທີມຜະລິດຕະພັນຈຳນວນຫຼາຍ ລວມທັງປະສົບການຂອງຜູ້ໃຊ້ (UX).

- **ພິຈາລະນາຜົນທີ່ຕາມມາຂອງປະສົບການຂອງຜູ້ໃຊ້ຈາກການຕັ້ງຄ່າຄວາມປອດໄພ.** ແຕ່ລະການຕັ້ງຄ່າໃໝ່ຈະເພີ່ມພາລະທາງດ້ານການຮັບຮູ້ໃຫ້ກັບຜູ້ໃຊ້ ແລະ ຄວນຈະໄດ້ຮັບການປະເມີນໂດຍສົມທົບກັບຜົນປະໂຫຍດທາງທຸລະກິດທີ່ໄດ້ຮັບ. ໂດຍຫຼັກການແລ້ວ ການຕັ້ງຄ່າບໍ່ຄວນມີຢູ່ ແຕ່ລວມການຕັ້ງຄ່າທີ່ປອດໄພທີ່ສຸດເຂົ້າໃນຜະລິດຕະພັນໂດຍຄ່າເລີ່ມຕົ້ນແທນ. ເມື່ອຈຳເປັນຕ້ອງມີການຕັ້ງຄ່າ ທາງເລືອກເລີ່ມຕົ້ນຄວນຈະມີຄວາມປອດໄພຢ່າງກວ້າງຂວາງຕໍ່ກັບໄພຂົ່ມຂູ່ທົ່ວໄປ.

ອົງກອນຜູ້ຂຽນຮັບຮູ້ວ່າການປ່ຽນແປງເຫຼົ່ານີ້ອາດຈະມີຜົນກະທົບຕໍ່ການດຳເນີນງານກ່ຽວກັບວິທີການເຮັດວຽກຂອງຊອັບແວ. ດັ່ງນັ້ນ ຂໍ້ມູນທີ່ໄດ້ຮັບຈາກລູກຄ້າແມ່ນມີສຳຄັນຢ່າງຍິ່ງໃນການສ້າງດຸ່ນດ່ຽງລະຫວ່າງການພິຈາລະນາການດຳເນີນງານ ແລະ ຄວາມປອດໄພ. ພວກເຮົາເຊື່ອວ່າການສ້າງແຜນງານທີ່ເປັນລາຍລັກອັກສອນ ແລະ ການສະໜັບສະໜູນຜູ້ບໍລິຫານທີ່ຈັດລຳດັບຄວາມສຳຄັນຂອງແນວຄວາມຄິດເຫຼົ່ານີ້ເຂົ້າໄປໃນຜະລິດຕະພັນທີ່ສຳຄັນຂອງອົງກອນເປັນບາດກ້າວທຳອິດໃນການຫັນປ່ຽນໄປສູ່ແນວປະຕິບັດການພັດທະນາ ຊອັບແວທີ່ປອດໄພ. ເຖິງແມ່ນວ່າການປ້ອນຂໍ້ມູນຂອງລູກຄ້າມີຄວາມສຳຄັນ ແຕ່ພວກເຮົາກໍໄດ້ສັງເກດເຫັນກໍລະນີທີ່ສຳຄັນທີ່ລູກຄ້າບໍ່ເຕັມໃຈ ຫຼື ບໍ່ສາມາດຮັບຮອງເອົາມາດຕະຖານທີ່ໄດ້ຮັບການປັບປຸງມາໃຊ້ ຊຶ່ງມັກຈະເປັນໂປຣໂຕຄອນເຄືອຂ່າຍ. ມັນເປັນສິ່ງສຳຄັນສຳລັບຜູ້ຜະລິດໃນການສ້າງແຮງຈູງໃຈທີ່ມີຄວາມໝາຍສຳລັບລູກຄ້າໃຫ້ທັນສະໄໝ ແລະ ບໍ່ອະນຸຍາດໃຫ້ພວກເຂົາຕົກຢູ່ໃນຄວາມສ່ຽງທີ່ບໍ່ມີກຳນົດ.

ຄູ່ມືການແຂງຕົວ ແລະ ຄູ່ມືການຄາຍຕົວ

ຄູ່ມືການແຂງຕົວອາດຈະເປັນຜົນມາຈາກການຂາດການຄວບຄຸມຄວາມປອດໄພຂອງຜະລິດຕະພັນຖືກຝັງເຂົ້າໄປໃນສະຖາປັດຕະຍະກຳ ຂອງຜະລິດຕະພັນຕັ້ງແຕ່ເລີ່ມຕົ້ນຂອງການພັດທະນາ. ດັ່ງນັ້ນ ຄູ່ມືການແຂງຕົວຈຶ່ງອາດເປັນແຜນງານສຳລັບຝ່າຍກົງກັນຂ້າມໃນການ ລະບຸໃຫ້ເຫັນ ແລະ ໃຊ້ປະໂຫຍດຈາກຄຸນສົມບັດທີ່ບໍ່ປອດໄພ. ມັນເປັນເລື່ອງປົກກະຕິທີ່ຫຼາຍອົງກອນຈະບໍ່ຮູ້ຈັກຄູ່ມືການແຂງຕົວ ດັ່ງນັ້ນ ພວກເຂົາຈຶ່ງປ່ອຍໃຫ້ການຕັ້ງຄ່າການກຳນົດຄ່າອຸປະກອນຢູ່ໃນສະຖານະທີ່ບໍ່ປອດໄພ. ຮູບແບບຈຳລອງກັບທາງ ທີ່ຮູ້ຈັກກັນວ່າເປັນຄູ່ມື ການຄາຍຕົວຄວນແທນທີ່ຄູ່ມືການແຂງຕົວດັ່ງກ່າວ ແລະ ອະທິບາຍວ່າການປ່ຽນແປງໃດທີ່ຜູ້ໃຊ້ຄວນເຮັດໃນຂະນະດຽວກັນກໍຍັງສະແດງ ລາຍການຄວາມສ່ຽງດ້ານຄວາມປອດໄພທີ່ເກີດຂຶ້ນດ້ວຍ. ຄູ່ມືເຫຼົ່ານີ້ຄວນຈະຖືກຂຽນໂດຍຜູ້ປະຕິບັດງານດ້ານຄວາມປອດໄພທີ່ສາມາດ ອະທິບາຍຂໍ້ດີ ແລະ ຂໍ້ເສັຍດ້ວຍພາສາທີ່ຊັດເຈນເພື່ອເພີ່ມໂອກາດທີ່ຈະຖືກນຳໃຊ້ຢ່າງຖືກຕ້ອງ.

ແທນທີ່ຈະພັດທະນາຄູ່ມືການແຂງຕົວຊຶ່ງລະບຸວິທີການຮັກສາຄວາມປອດໄພຂອງຜະລິດຕະພັນ ອົງກອນຜູ້ຂຽນແນະນຳໃຫ້ຜູ້ຜະລິດ ຊອັບແວປ່ຽນໄປໃຊ້ແນວທາງທີ່ປອດໄພໂດຍວິທີການເລີ່ມຕົ້ນ ແລະ ສະໜອງ "ຄູ່ມືການຄາຍຕົວ." ຄູ່ມືເຫຼົ່ານີ້ອະທິບາຍຄວາມສ່ຽງທາງ ທຸລະກິດໃນການຕັດສິນໃຈດ້ວຍພາສາທຳມະດາທີ່ເຂົ້າໃຈໄດ້ງ່າຍ ແລະ ສາມາດສ້າງຄວາມຮັບຮູ້ຂອງອົງກອນກ່ຽວກັບຄວາມສ່ຽງຕໍ່ການ ບຸກລຸກທາງໄຊເບີທີ່ເປັນອັນຕະລາຍ. ຂໍ້ດີ ແລະ ຂໍ້ເສັຍຄວນຈະຖືກກຳນົດໂດຍຜູ້ບໍລິຫານລະດັບສູງຂອງລູກຄ້າ, ເພື່ອສ້າງຄວາມດຸ່ນດ່ຽງ ລະຫວ່າງຄວາມປອດໄພກັບຂໍ້ກຳນົດທາງທຸລະກິດອື່ນໆ.

ຄຳແນະນຳສຳລັບລູກຄ້າ

ອົງກອນຜູ້ຂຽນແນະນຳອົງກອນຕ່າງໆໃຫ້ຜູ້ຜະລິດຊອັບແວທີ່ຈັດຫາຂອງພວກເຂົາຮັບຜິດ ຊອບຕໍ່ຜົນ ໄດ້ຮັບດ້ານຄວາມປອດໄພຂອງຜະລິດຕະພັນຂອງຕົນ. ສ່ວນໜຶ່ງຂອງສິ່ງນີ້ ອົງກອນຜູ້ຂຽນແນະນຳໃຫ້ ຜູ້ບໍລິຫານຈັດລຳດັບຄວາມສຳຄັນຂອງການຈັດຊື້ຜະລິດຕະພັນທີ່ປອດໄພໂດຍການອອກແບບ ແລະ ປອດໄພໂດຍຄ່າເລີ້ມຕົ້ນ. ສິ່ງນີ້ສາມາດສະແດງໃຫ້ເຫັນໄດ້ໂດຍຜ່ານການສ້າງນະໂຍບາຍທີ່ກຳນົດໃຫ້ພະແນກ ໄອທີ ປະເມີນຄວາມປອດໄພຂອງຊອັບແວກ່ອນທີ່ຈະຊື້ ເຊັ່ນດຽວກັນກັບການມອບອຳນາດໃຫ້ພະແນກ ໄອທີ ທີ່ສາມາດຖອຍກັບຄືນໄດ້ຖ້າຈຳເປັນ. ພະແນກ ໄອທີ ຄວນໄດ້ຮັບອຳນາດໃນການພັດທະນາເງື່ອນໄຂ ການຈັດຊື້ທີ່ເນັ້ນໜັກເຖິງຄວາມສຳຄັນຂອງແນວປະຕິບັດຂອງ ຄວາມປອດໄພໂດຍການອອກແບບ ແລະ ຄວາມ ປອດໄພໂດຍຄ່າເລີ້ມຕົ້ນ (ທັງທີ່ໄດ້ກ່າວໄວ້ໃນເອກະສານນີ້ ແລະ ອື່ນໆທີ່ພັດທະນາໂດຍ ອົງກອນ). ນອກຈາກນັ້ນ, ພະແນກ ໄອທີ ຄວນໄດ້ຮັບການສະໜັບສະໜູນຈາກຝ່າຍບໍລິຫານໃນເວລາທີ່ບັງຄັບໃຊ້ ເງື່ອນໄຂເຫຼົ່ານີ້ໃນການຕັດສິນໃຈຊື້. ການຕັດສິນໃຈຂອງອົງກອນທີ່ຈະຍອມຮັບຄວາມສ່ຽງທີ່ກ່ຽວຂ້ອງກັບ ຜະລິດຕະພັນເທັກໂນໂລຢີສະເພາະຄວນໄດ້ຮັບການບັນທຶກຢ່າງເປັນທາງການ ອະນຸມັດໂດຍຜູ້ບໍລິຫານ ທຸລະກິດລະດັບສູງ ແລະ ນຳສະເໜີຢ່າງເປັນປະຈຳຕໍ່ຄະນະກຳມະການບໍລິຫານ.

ການບໍລິການ ໄອທີ ທີ່ສຳຄັນຂອງວິສາຫະກິດທີ່ສະໜັບສະໜູນມາດຕະການ ຮັກສາຄວາມປອດໄພຂອງ ອົງກອນ ເຊັ່ນ ເຄືອຂ່າຍ ວິສາຫະກິດ ຂໍ້ມູນປະຈຳຕົວວິສາຫະກິດ ແລະ ການຄຸ້ມຄອງການເຂົ້າເຖິງ ແລະ ການດຳເນີນງານດ້ານຄວາມປອດໄພ ແລະ ຄວາມສາມາດໃນການຕອບສະໜອງຄວນຈະໄດ້ຮັບການເບິ່ງເຫັນ ວ່າເປັນໜ້າທີ່ທາງທຸລະກິດທີ່ສຳຄັນຊຶ່ງໄດ້ຮັບທຶນເພື່ອໃຫ້ສອດຄ່ອງກັບຄວາມສຳຄັນຂອງເຂົາເຈົ້າກັບຜົນສຳ ເລັດຂອງພາລະກິດຂອງອົງກອນ. ອົງກອນຄວນພັດທະນາແຜນການເພື່ອຍົກລະດັບຄວາມສາມາດເຫຼົ່ານີ້ ເພື່ອຊຸກຍູ້ຜູ້ຜະລິດທີ່ຍອມຮັບຄວາມປອດໄພໂດຍການອອກແບບ ແລະ ຄວາມປອດໄພໂດຍຄ່າເລີ້ມຕົ້ນ.

ຖ້າເປັນໄປໄດ້, ອົງກອນຕ່າງໆ ຄວນພະຍາຍາມສ້າງຄວາມສຳພັນທາງຍຸດທະສາດກັບຜູ້ສະໜອງດ້ານໄອທີ ທີ່ສຳຄັນຂອງຕົນ ສາຍພົວພັນດັ່ງກ່າວປະກອບມີຄວາມໄວ້ວາງໃຈໃນຫຼາຍລະດັບຂອງອົງກອນ ແລະ ເປັນ ຊ່ອງທາງໃນການແກ້ໄຂບັນຫາ ແລະ ກຳນົດຄວາມສຳຄັນຮ່ວມກັນ. ຄວາມປອດໄພຄວນຈະເປັນອົງປະກອບ ທີ່ສຳຄັນຂອງຄວາມສຳພັນດັ່ງກ່າວ ແລະ ອົງກອນຄວນພະຍາຍາມເສີມສ້າງຄວາມສຳຄັນຂອງແນວປະຕິບັດ ຄວາມປອດໄພໂດຍການອອກແບບ ແລະ ຄວາມປອດໄພໂດຍການຕັ້ງຄ່າໃນທັງສອງມິຕິທີ່ເປັນທາງການ (ເຊັ່ນ ສັນຍາ ຫຼື ຂໍ້ຕົກລົງຜູ້ຂາຍ) ແລະ ມິຕິທີ່ບໍ່ເປັນທາງການຂອງຄວາມສຳພັນ. ອົງກອນຄວນຄາດ ຫວັງຄວາມໂປ່ງໃສຈາກຜູ້ສະໜອງເທັກໂນໂລຢີຂອງພວກເຂົາກ່ຽວກັບຈຸດຢືນການຄວບຄຸມພາຍໃນຂອງ ພວກເຂົາເຊັ່ນດຽວກັນກັບແຜນງານຂອງພວກເຂົາໄປສູ່ການຮັບຮອງເອົາແນວປະຕິບັດດ້ານຄວາມປອດໄພ ໂດຍການອອກແບບ ແລະ ຄວາມປອດໄພໂດຍຄ່າເລີ້ມຕົ້ນ.

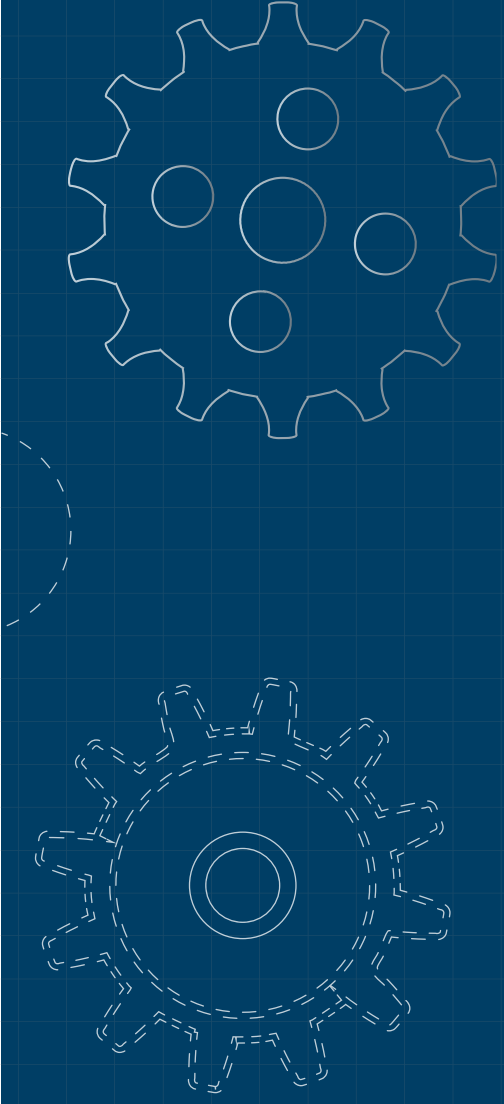
ນອກເໜືອໄປຈາກການສ້າງຄວາມປອດໄພໂດຍຄ່າເລີ່ມຕົ້ນເປັນບູລິມະສິດພາຍໃນອົງກອນແລ້ວ ຜູ້ນຳດ້ານໄອທີຄວນຮ່ວມມືກັບເພື່ອນຮ່ວມງານໃນອຸດສາຫະກຳຂອງພວກເຂົາເພື່ອທຳຄວາມເຂົ້າໃຈວ່າຜະລິດຕະພັນ ແລະ ບໍລິການໃດທີ່ເໝາະສົມກັບຫຼັກການອອກແບບເຫຼົ່ານີ້ໄດ້ດີທີ່ສຸດ. ຜູ້ນຳເຫຼົ່ານີ້ຄວນປະສານການຮ້ອງຂໍຂອງພວກເຂົາເພື່ອຊ່ວຍໃຫ້ຜູ້ຜະລິດຈັດລຳດັບຄວາມສຳຄັນຂອງການລິເລີ່ມດ້ານຄວາມປອດໄພທີ່ຈະເກີດຂຶ້ນຂອງພວກເຂົາ. ໂດຍການເຮັດວຽກຮ່ວມກັນ ລູກຄ້າສາມາດຊ່ວຍສະໜອງການປ້ອນຂໍ້ມູນທີ່ມີຄວາມໝາຍໃຫ້ແກ່ຜູ້ຜະລິດ ແລະ ສ້າງແຮງຈູງໃຈໃຫ້ພວກເຂົາຈັດລຳດັບຄວາມສຳຄັນຂອງຄວາມປອດໄພໄດ້.

ເມື່ອນຳໃຊ້ລະບົບຄລາວດ, ອົງກອນຄວນຮັບປະກັນວ່າພວກເຂົາເຂົ້າໃຈຮູບແບບຄວາມຮັບຜິດຊອບຮ່ວມກັນກັບຜູ້ສະໜອງເຕັກໂນໂລຢີຂອງພວກເຂົາ. ນັ້ນຄື ອົງກອນຄວນມີຄວາມຊັດເຈນກ່ຽວກັບຄວາມຮັບຜິດຊອບດ້ານຄວາມປອດໄພຂອງຜູ້ສະໜອງແທນທີ່ຈະເປັນພຽງຄວາມຮັບຜິດຊອບຂອງລູກຄ້າເທົ່ານັ້ນ.

ອົງກອນຄວນຈັດລຳດັບຄວາມສຳຄັນຂອງຜູ້ໃຫ້ບໍລິການລະບົບຄລາວດ໌ທີ່ມີຄວາມໂປ່ງໃສກ່ຽວກັບມາດຕາການຄວາມປອດໄພ ການຄວບຄຸມພາຍໃນ ແລະ ຄວາມສາມາດໃນການປະຕິບັດຕາມພັນທະຂອງພວກເຂົາພາຍໃຕ້ຮູບແບບຄວາມຮັບຜິດຊອບຮ່ວມກັນ.

ຂໍ້ຈຳກັດຄວາມຮັບຜິດຊອບ

ຂໍ້ມູນໃນບົດລາຍງານນີ້ແມ່ນໄດ້ຖືກຈັດທຳຂຶ້ນ "ຕາມສະພາບ" ເພື່ອຈຸດປະສົງໃນການໃຫ້ຂໍ້ມູນຂ່າວສານເທົ່ານັ້ນ. CISA ແລະ ອົງກອນຜູ້ຂຽນບໍ່ຮັບຮອງຜະລິດຕະພັນ ຫຼື ການບໍລິການທາງການຄ້າໃດໆ, ລວມເຖິງຫົວຂໍ້ໃດໜຶ່ງຂອງການວິເຄາະ. ການອ້າງອີງເຖິງຫົວໜ່ວຍງານທາງການຄ້າສະເພາະ ຫຼື ຜະລິດຕະພັນການຄ້າ, ຂະບວນການ ຫຼື ການບໍລິການໂດຍເຄື່ອງໝາຍການບໍລິການ, ເຄື່ອງໝາຍການຄ້າ, ຜູ້ຜະລິດ ຫຼື ອື່ນໆບໍ່ຖືເປັນ ຫຼື ບໍ່ດັ່ງນັ້ນບໍ່ໄດ້ປະກອບ ຫຼື ໝາຍເຖິງການຮັບຮອງ, ການແນະນຳ ຫຼືການນິຍົມ ໂດຍ CISA ແລະ ອົງກອນຜູ້ຂຽນ. ເອກະສານນີ້ແມ່ນຄວາມຄິດລິເລີ່ມຮ່ວມກັນຂອງ CISA ທີ່ບໍ່ໄດ້ເຮັດໜ້າທີ່ໃຫ້ບໍລິການເປັນເອກະສານລະບຽບກຳກັບດູແລໂດຍອັດຕະໂນມັດ.



ແຫ່ງຂໍ້ມູນ

CISA ຊີໄອເອັສເອ

- » ຄຳແນະນຳ SBOM ຂອງ CISA
- » ເປົ້າໝາຍປະສິດທິພາບດ້ານຄວາມປອດໄພທາງໄຊເບີຂ້າມຂະແໜງຂອງ CISA
- » ແນວທາງຊີ້ນຳກ່ຽວກັບການເຮັດວຽກຮ່ວມກັນດ້ານເທັກໂນໂລຢີ
- » ການປ້ອງກັນການໂຈມຕີລະບົບຕ່ອງໂສ້ການສະໜອງຊອບແວຂອງ CISA ແລະ NIST
- » ຄ່າໃຊ້ຈ່າຍຂອງເທັກໂນໂລຢີທີ່ບໍ່ປອດໄພ ແລະ ສິ່ງທີ່ພວກເຮົາສາມາດເຮັດໄດ້ກ່ຽວກັບເທັກໂນໂລຢີດັ່ງກ່າວ | CISA
- » ຢຸດການເບິ່ງຂ້າມເລື້ອງຄວາມປອດໄພທາງໄຊເບີ: ເປັນຫຍັງບໍລິສັດຕ່າງໆຈຶ່ງຕ້ອງສ້າງຄວາມປອດໄພໃຫ້ກັບຜະລິດຕະພັນເທັກໂນໂລຢີ (foreignaffairs.com)
- » ຄຳແນະນຳການຈັດປະເພດຊ່ອງໂຫວ່ສະເພາະຜູ້ມີສ່ວນກ່ຽວຂ້ອງຂອງ CISA (SSVC)
- » ເອກະສານຂໍ້ເທັດຈິງ MFA ກ່ຽວກັບການຕໍ່ຕ້ານ ຟິຊຊິ່ງ ຂອງ CISA
- » ຄຳແນະນຳທາງໄຊເບີສຳລັບທຸລະກິດຂະໜາດນ້ອຍ | CISA

NSA ເອັນເອັສເອ

- » ເອກະສານຂໍ້ມູນຄວາມປອດໄພທາງໄຊເບີຂອງ NSA ກ່ຽວກັບຄວາມປອດໄພຂອງໜ່ວຍຄວາມຈຳ
- » ESF ຂອງ NSA ໃນການຮັກສາຄວາມປອດໄພລະບົບຕ່ອງໂສ້ການສະໜອງຊອບແວ: ແນວປະຕິບັດທີ່ດີທີ່ສຸດສຳລັບຜູ້ສະໜອງ

FBI FBI ເອັຟບີໄອ

- » ຄວາມເຂົ້າໃຈ ແລະ ການຕອບໂຕ້ການໂຈມຕີລະບົບຕ່ອງໂສ້ການສະໜອງ SolarWinds: ທັດສະນະຂອງລັດຖະບານກາງ
- » ໄພຂົ່ມຂູ່ທາງໄຊເບີ - ການຕອບສະໜອງ ແລະ ການລາຍງານ
- » ວຸດທະວິທີທາງໄຊເບີຂອງ FBI

ສະຖາບັນມາດຕະຖານ ແລະ ເທັກໂນໂລຢີແຫ່ງຊາດ (NIST)

- » ແນວທາງຊີ້ນຳການລະບຸຕົວຕົນດິຈິຕອນຂອງ NIST
- » ກອບວຽກດ້ານຄວາມປອດໄພທາງໄຊເບີຂອງ NIST
- » ໂຄງຮ່າງການພັດທະນາຊອບແວທີ່ປອດໄພຂອງ NIST (SSDF)

ສູນຮັກສາຄວາມປອດໄພທາງໄຊເບີຂອງອອສເຕຣເລັຍ (ACSC)

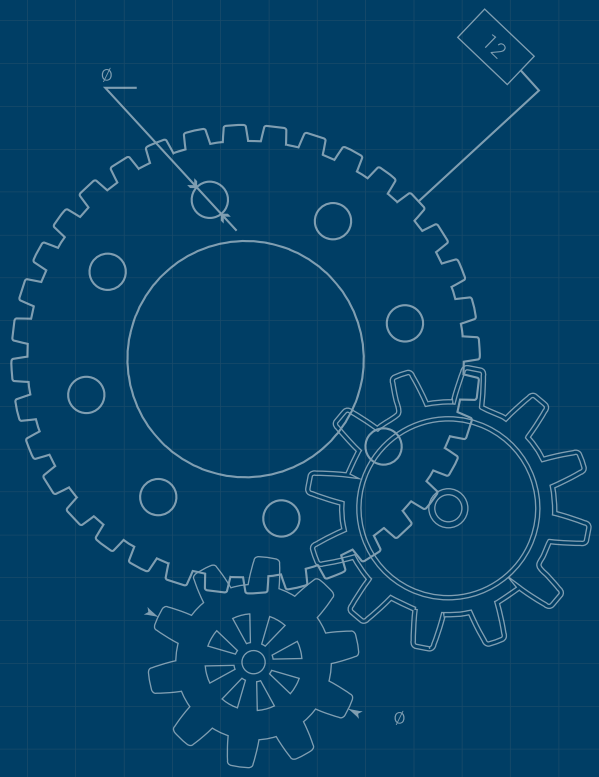
- » ຂໍ້ແນະນຳການປະຕິບັດລະຫັດ IoT ຂອງ ACSC ສຳລັບຜູ້ຜະລິດ

ສູນຄວາມປອດໄພທາງໄຊເບີແຫ່ງຊາດຂອງຣາດຊະອານາຈັກ (UK)

- » ຂອບການປະເມີນທາງໄຊເບີຂອງຣາດຊະອານາຈັກ
- » ຄຳແນະນຳດ້ານການພັດທະນາ ແລະ ການນຳໃຊ້ທີ່ປອດໄພຂອງ UK NCSC
- » ຄຳແນະນຳດ້ານການຄຸ້ມຄອງຄວາມສ່ຽງຂອງ UK NCSC
- » ຊຸດເຄື່ອງມືເປີດເຜີຍຊ່ອງໂຫວ່ຂອງ NCSC ຂອງຣາດຊະອານາຈັກ
- » CHERI ຂອງ ມະຫາວິທະຍາໄລ ແຄມບຣິດຈ໌
- » ເປັນເວລາດົນນານ ແລະ ຂອບໃຈສຳລັບຂໍ້ມູນທັງໝົດ - NCSC.GOV.UK

ສູນຄວາມປອດໄພທາງໄຊເບີຂອງການາດາ (CCCS)

- » ຄຳແນະນຳການປະຕິບັດ ຂອງ CCCS ກ່ຽວກັບການປ້ອງກັນການໂຈມຕີລະບົບຕ່ອງໂສ້ການສະໜອງຊອບແວ
- » ຕ່ອງໂສ້ການສະໜອງທາງໄຊເບີ: ວິທີການປະເມີນຄວາມສ່ຽງ
- » ແນວທາງຊີ້ນຳ ກ່ຽວກັບ CONTI ແຮນຊຳແວ ຂອງສູນການາດາເພື່ອຄວາມປອດໄພທາງໄຊເບີ



ສຳນັກງານຄວາມປອດໄພຂໍ້ມູນຂ່າວສານຂອງເຢັຍຣະມັນ (BSI)

» ບົດສະຫຼຸບ BSI Grundschutz (ໂມດູນ CON.8)
» ມາດຕະຖານສາກົນ IEC 62443, ພາກທີ 4-1
» ລາຍງານສະຖານະຄວາມປອດໄພດ້ານໄອທີ ໃນ ເຢັຍລະມັນ ປີ 2022
» ແນວປະຕິບັດ BSI ຂອງຄວາມປອດໄພ ຂອງ ແອັບພລິເຄຊັນເວັບ

ສູນຄວາມປອດໄພທາງໄຊເບີແຫ່ງຊາດ ຂອງ ເນເທີແລນດ໌ (NCSC-NL)

» ເອກະສານການຢັ້ງຢືນຄວາມຖືກຕ້ອງສະບັບສົມບູນ ຂອງ NCSC-NL

ສູນກຽມຄວາມພ້ອມດ້ານອຸປະຕິເຫດ ແລະ ຍຸດທະສາດ ແຫ່ງຊາດ ຂອງ ຍີ່ປຸ່ນ ເພື່ອຄວາມປອດໄພທາງໄຊເບີ (NISC)

» ຍຸດທະສາດຄວາມປອດໄພທາງໄຊເບີແຫ່ງຊາດຂອງຍີ່ປຸ່ນ

ກະຊວງເສດຖະກິດ ການຄ້າ ແລະ ອຸດສາຫະກຳ ຂອງ ຍີ່ປຸ່ນ (METI)

» ຄຳແນະນຳເບື້ອງຕົ້ນ ກ່ຽວກັບລາຍການວັດສະດຸຊ້ອນແວ(SBOM) ສຳລັບການຄຸ້ມຄອງຊອັບແວ
» ການລວບລວມຕົວຢ່າງກໍລະນີການນຳໃຊ້ກ່ຽວກັບວິທີການຄຸ້ມຄອງສຳລັບການນຳໃຊ້ OSS ແລະ ການຮັບປະກັນຄວາມປອດໄພ

ສຳນັກງານຄວາມໝັ້ນຄົງທາງໄຊເບີ ຂອງ ສິງກະໂປ

» ທີ່ປຶກສາດ້ານວິຊາການກ່ຽວກັບການພັດທະນາ API ທີ່ປອດໄພ
» ນະໂຍບາຍການເປີດເຜີຍຊ່ອງໂຫວ່ ຂອງ CSA SingCERT
» ລາຍການກວດສອບການຕອບໂຕ້ຕໍ່ເຫດການຂອງ CSA SingCERT
» ຄູ່ມືການຕອບໂຕ້ຕໍ່ເຫດການ ຂອງ CSA SingCERT
» ຄວາມປອດໄພຂອງ CSA ຕາມກອບວຽກງານການອອກແບບ
» ລາຍການກວດສອບຄວາມປອດໄພຂອງ CSA ຕາມກອບວຽກງານການອອກແບບ
» ຄູ່ມື CSA ກ່ຽວກັບການສ້າງແບບຈຳລອງໄພຂົ່ມຂູ່ທາງໄຊເບີ
» ໂຄງການຕິດປ້າຍກຳກັບຄວາມປອດໄພທາງໄຊເບີ ຂອງ CSA

ອື່ນໆ

» ລະບົບທີ່ຊັບຊ້ອນລົ້ມເຫຼວແນວໃດ
» ລັກສະນະໃໝ່ໃນຄວາມລົ້ມເຫຼວຂອງລະບົບທີ່ຊັບຊ້ອນ

ເອກະສານອ້າງອີງ

[1] https://csrc.nist.rip/publications/history/ande72.pdf

[2] https://www.cisa.gov/sbom ແລະ SBOMs ອ້າງອີງໃນ TR 03183-2 https://www.bsi.bund.de/dok/TR-03183

[3] Juran ເລື້ອງຄຸນນະພາບໂດຍການອອກແບບໂດຍ J.M. Juran, 1992.