TLP:CLEAR

ဆိုက်ဘာလုံခုံရြေးအနှတရာယ်ဆိုင်ရာဟန်ချက် ပြောင်းလဲခငြ်း – လုံခုံရြေးရှိရန် ပငြ်ဆင်စီမံ လုပ်ဆောင်ခငြ်းနှင့် အလိုအလျောက် လုံခုံခြေသေခေအနအေထား ဖစြ်စခေငြ်းအတွက် အခငြခံသဘောတရားနှင့် ကိုင်တွယ်ဖငြရှင်းနည်းများ

ထုတ်ဝသေည့်ရက် – ဧပြေီ၃၊ ၂၀၂၃

ဆိုက်ဘာလုံခုံရြေးနှင့် အခငြခံအဆောက်အဦး လုံခုံရြေးဆိုင်ရာ အဂျေင်စီ

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

မာတိကာဇယား

မာတိကာဇယား 2

အကျဉ်းချုံး – လုံခုံမြဲ အားနည်းသော ပင်ဆင်မှု 3

လုံခုံမြဲရှိအောင် ပင်ဆင်စီမံခင်း 5

လုံခုံမြဲရှိအောင် ပင်ဆင်စီမံခင်း 7

ဆင့်ဖဲ့ထဲ ထုတ်လုပ်သူများအတွက် အကံပြုချက်များ 8

ဆင့်ဖဲ့ထဲ ကုန်ပစ္စည်းများအတွက် လုံခုံရေးဆိုင်ရာ အခြေခံမူများ 8

လုံခုံမြဲရှိအောင် ပင်ဆင်စီမံခင်း၏ ဗျူဟာများ 11

အလိုအလျောက် လုံခုံမြဲရှိနေခင်း ၏ ဗျူဟာများ 14

တင်းကျပ်မှု နှင့် ဖြေလျှော့မှု လမ်းညွှန်များ Hardening Vs Loosening Guides 17

ဝယ်ယူသုံးစွဲသူများအတွက် အကံပြုချက်များ 17

မသက်ဆိုင်ကြောင်းရှင်းလင်းချက် 19

ကျမ်းကိုးစာများ 19

အကျဉ်းချုံး – လုံခုံမြဲအားနည်းသော ပင်ဆင်မှု

စက်မှုနည်းပညာသည် နိစ္စစဆုဝဘဝ၏ ဘက်ပေါင်းစုံတွင် ပါဝင်ပေါင်းစပ်မှုရှိနေပါသည်။ အင်တာနက်ကို အခြေခံသည့်စနစ်များသည် ကျွန်ုပ်တို့၏ စီးပွားရေးဖွံ့ဖိုးတိုးတက်ရေး၊ ရှင်သန်နထိုင်မှုများနှင့် ကျန်းမာရေးအပြင် ကိုယ်ရေးအချက်အလက် စီမံခန့်ခွဲရေးမှစ၍ ကျန်းမာရေးစောင့်ရှောက်မှုအထိ တိုက်ရိုက်သက်ရောက်မှုရှိသော အရေးကြီးသည့် စနစ်များနှင့် ချိတ်ဆက်မှုရှိနေပါသည်။ ဥပမာတစ်ခု ပရမည်ဆိုလျင် – ဆိုက်ဘာလုံခုံရေးများ ချိုးဖောက်ခံရသောကြောင့် ဆေးရုံများတွင် ခွဲစိတ်မှုများကို ဖျက်သိမ်းလိုက်ရခြင်းများနှင့် တကမ္ဘာလုံး၏ လူနာစောင့်ရှောက်ရေးတွင် အပြောင်းအလဲများ ဖစ်စေပါသည်။ နည်းပညာ လုံခုံမြဲမရှိခြင်းနှင့် အရေးကြီးသည့် အချက်အလက်သိုလှောင်ရေးစနစ်များတွင် အားနည်းချက်များ ရှိခြင်းသည် မသမာသည့် ဆိုက်ဘာကျူးကျော်တိုက်ခိုက်မှုများ ဖစ်စေရန် ဖိတ်ခေါ်သလို ဖစ်စေနိုင်ပြီးထိုမှတဆင့် ဆိုးဝါးသည့် လုံခုံရေး[1] ဆိုင်ရာ အန္တရာယ်များ ကျရောက်စေနိုင်ပါသည်။

ယခင်ကထက် ယခုအချိန်တွင် စက်မှုကုန်ထုတ်လုပ်သူများအတွက် မိမိ၏ ထုတ်ကုန်များထုတ်လုပ်သည့်အခါတွင် လုံခုံမြဲရှိအောင် ပင်ဆင်စီမံလုပ်ဆောင်ခြင်း Secure-by-Design နှင့် အလိုအလျောက် လုံခုံမြဲရှိနခြင်းများ Secure-by-Default ကို အဓိကထားပြီးလုံခုံဖြာရှိအောင် မွမ်းမံထားသည့် ပစ္စည်းများကို ထုတ်လုပ်ရန် အင်မတန်မှ အရေးကြီးပါသည်။ တချို့ထုတ်လုပ်သူများသည် ဆင့်ဖဲ့ဝဲလုံခုံမြဲရှိအောင် တိုးတက်သဘောခြလှမ်းများနှင့် လုပ်ဆောင်နပေါ်ပြီ တချို့ထုတ်လုပ်သူများမှာ နဂောက်ကျကျန်နတောမျိုး ဖစ်နပေါသည်။ အာဏာပိုင်များအနဖေါ့ စက်မှုကုန်ထုတ်လုပ်သူတိုင်းအား အကံပြုလိုသည်မှာ မိမိ၏ ထုတ်ကုန်ပစ္စည်းများကို ထုတ်လုပ်ရာတွင် ဆိုက်ဘာကျူးကျော်တိုက်ခိုက်မှမှ ကာကွယ်ရန်အတွက် သုံးစွဲသူများမှ တချိန်လုံး စောင့်ကပြမှလုပ်ရခြင်း၊ မကြာခဏ အသစ်မွမ်းမံရခြင်း၊ ပင်ဆင်ရခြင်းမျိုး ပုံပြုပ်စရာမလိုအောင် ဆောင်ရွက်ကရန် အကံပြုလိုပါသည်။ သုံးစွဲသူများအတွက် လုံခုံမြဲပိုကောင်းမွန်စရေးအတွက် ကုန်ထုတ်လုပ်သူဖက်မှ တာဝန်ယူလုပ်ဆောင်ပေးရန် အကံပြုလိုပါသည်။ ယခင်ကဆိုလျင် သုံးစွဲသူများမှ ပစ္စည်းကို ဝယ်ယူသုံးစွဲပြီးမှ တွေ့ရှိသည့် အားနည်းချက်များကို ကုန်ထုတ်လုပ်သူများက ပင်ဆင်ပေးခြင်းဖစ်ပြီး ကုန်ထုတ်လုပ်သူများက အမှားကိုပင်ဆင်သည့်အခါတွင်လည်း သုံးစွဲသူများမှ အဖိုးအခများထပ်မံ အကုန်အကျခံခဲ့ရသည့် အနအေထားရှိခဲ့ပါသည်။ ကုန်မထုတ်လုပ်မီအချိန်မှစ၍ လုံခုံမြဲရှိရန် ပင်ဆင်စီမံမှုနည်းဖဖြ ထုတ်လုပ်မှသာလျင် တီထွင်လိုက် ပင်ဆင်လိုက်၊ ပန်ြတီထွင်လိုက်စသည့် သံသရာမှ ကင်းလွတ်နိုင်မည် ဖစ်ပါသည်။

အဆင့်မငြ်သည့် ဆင့ဖဲ့ဝဲလုံခုံရေး ရရှိရန်အတွက် ကုန်ထုတ်လုပ်သူများအနဖေါ့ ဈေးကွက်တွင် မရောင်းချမီ လုံခုံရေးကို ရှေးရှုပေါင်းစပ်ထားသည့် ကုန်ပစ္စည်းများကို လုပ်ဆောင်ရန်လိုအပ်သည်ဟု နှလုံးသွင်းပြီးဦးစားပေးလုပ်ဆောင်ပေးရန် အာဏာပိုင်အဖျေါ်စီများအနဖေါ့ အကံပြုလိုပါသည်။ အချိန်ကြာလာသည်နှင့်အမျှ အင်ဂျင်နီယာအဖွဲ့များသည် လုံခုံမြဲရှိသည့် ကုန်ပစ္စည်းများအား

[1] "လုံခုံမြဲ" ဟု ဆိုရာတွင် အကြောင်းအရာအပေါ်မူတည်၍ အဓိပ္ပာယ် အမျိုးမျိုးဆောင်နိုင်ကြောင်း အာဏာပိုင်အဖျေါ်စီများ အသိအမှတ်ပြုပါသည်။ ယခုလမ်းညွှန်မှုအတွက် 'လုံခုံမြဲ' ဟု ဆိုရာတွင် ဝယ်ယူသုံးစွဲသူများအား ဆိုက်ဘာတိုက်ခိုက်မှုများမှ ကာကွယ်ပေးနိုင်ရန် စက်မှုပိုင်းဆိုင်ရာ လုံခုံရေးအဆင့်အတန်းကို မဖြိတင်ခြင်းကို ရည်ညွှန်းပါသည်။

အားသွန်ခွန်စိုက်ထုတ်လုပ်စရာ မလိုပဲ အလိုအလျောက် ပုံမှန်အနအေထားအတိုင်း စည်းဝါးတကျ
လုပ်ဆောင်လာနိုင်ကမြည်ဖစ်ပြီးမွမ်းမံထိန်းသိမ်းမှု လုပ်ရခငြိးများလည်း
အားသွန်ခွန်စိုက်လုပ်ရန်မလိုအပ်သော အနအေထား ဖစ်လာနိုင်ပါသည်။ ထိုအချက်ကို ရှေးရှု၍
ဥရောပသမဂ္ဂသည် လုံခုံမြှရှိသည့် ကုန်ပစ္စည်းများထုတ်လုပ်ရန် အရေးကီးကြောင်းကို
တွန်းအားပေးသည့်အနဖေငြ့် ဆိုက်ဘာတိုက်ခိုက်ခငြိးကို ခုခံနိုင်ရေးအက်ဥပဒေ Cyber-Resilience-Act ကို
ရေးဆွဲခဲ့ပါသည်။ ထိုဆိုက်ဘာအက်ဥပဒသေည် လုံခုံမြှအားနည်းချက်ရှိနသေည့်
ကုန်ပစ္စည်းများစွေးကွက်တွင် မရှိစရေန်အတွက် ကုန်ထုတ်လုပ်သူများအနဖေငြ့် ကုန်ပစ္စည်းတစ်ခု၏
သက်တမ်းတလျောက်တွင် လုံခုံမြှရှိနရေန် တီထွင်လုပ်ဆောင် ထည့်သွင်းရမည်ဟု သတ်မှတ်ထားပါသည်။

အနာဂတ်တွင် သုံးစွဲသူများအတွက် လုံခုံမြှရှိသည့် စက်မှုကုန်ပစ္စည်းနှင့် ဆက်စပ်ကုန်ပစ္စည်းများ
တီထွင်နိုင်ရန်အတွက် အာဏာပိုင်အဖွေဲစီများမှ ကုန်ပစ္စည်းထုတ်လုပ်ရောင်းချသူများအား ၎င်းတို့၏
ကုန်ပစ္စည်းများကို ပန်ြလည်မွမ်းမံပြီးပစ္စည်းထုတ်လုပ်ရာတွင် လုံခုံမြှရှိအောင် ပငြ်ဆင်စီမံထားသည့်
ကုန်ပစ္စည်းများ (Secure-by-Design)နှင့် အလိုအလျောက် လုံခုံမြှရှိနသေည့် ကုန်ပစ္စည်းများ (Secure-by-
Default)ကိုသာ ထုတ်လုပ်ရန်ခွင့်ပြုဖြို့ တိုက်တွန်းထားပြီးထိုမှတဆင့် သုံးစွဲမည့်သူများထံ ရောင်းချရန်
တိုက်တွန်းလိုပါသည်။ လုံခုံမြှအတွက်ပငြ်ဆင်စီမံထားသော ကုန်ပစ္စည်းများဆိုသည်မှာ စက်မှုပိုင်းဆိုင်ရာ
တစ်ခုတည်းသာမက သုံးစွဲသူများ၏ လုံခုံခြောကင်းမှုကိုပါ ပဓာနထားသည့် စီးပွားလုပ်ငန်းမျိုးဖစ်ပါသည်။
လုံခုံမြှရှိအောင် ပငြ်ဆင်စီမံထားသော ကုန်ပစ္စည်းထုတ်လုပ်မှ မစတင်မီကပင် ထို့အတွက်
ရည်ရွယ်ချက်ထားရှိပြီးလုပ်ဆောင်ရမည်ဖစ်ပါသည်။ အလိုအလျောက်လုံခုံမြှရှိနသေည့်
ကုန်ပစ္စည်းများဆိုသည်မှာ ပုပြငြ်မွမ်းမံမှ ထပ်လုပ်ရန်နှင့် ထပ်မံကုန်ကျခံစရာမလိုအပ်ပဲ
လုံခုံခြေးအလိုအလျောက်ပါရှိသော ကုန်ပစ္စည်းများ ဖစ်ပါသည်။ ၎င်းအခငြခံမှများ
ပဝေါင်းစည်းလိုက်သည့်အခါတွင် ကုန်ထုတ်လုပ်သူများအတွက် လုံခုံခြေးဆိုင်ရာ ဝန်ထုတ်ဝန်ပိုးများ
လျော့ကျစသေလို သုံးစွဲသူများအား သားကောင်အဖစြ်မှ ရှောင်ရှားစနိုင်ပြီးငြင်းတို့ကို ကုန်ပစ္စည်းသုံးစွဲရာတွင်
လွဲမှားစွာ ဖွဲ့စည်းထုတ်လုပ်ထားသောပစ္စည်း၊ အလွယ်နည်းဖငြ့် ပုငြုပ်ထားသောပစ္စည်းနှင့် အခငြး
ပဿနာများရှိသော ကုန်ပစ္စည်းများ ဝယ်ယူသုံးစွဲမိရာမှ မိမိ၏ လုံခုံခြေး ထိခိုက်နစ်နာမှုများ မဖစြ်အောင်
လျော့ချပေးရာ ရောက်နိုင်ပါသည်။

ဆိုက်ဘာလုံခုံခြေးနှင့် အခငြခံအဆောက်အဦးလုံခုံခြေးဆိုင်ရာ အဖွေဲစီ(CISA)၊ နိုင်ငံတော် လုံခုံခြေးဆိုင်ရာ
အဖွေဲစီ (NSA)၊ ဗဟိုထောက်လှမ်းရေးဌာန(FBI) နှင့် အောက်ပါ နိုင်ငံတကာ မိတ်ဖက်အဖွဲ့များ[2] သည်
ကုန်ထုတ်လုပ်သူများအနဖေငြ့် ၎င်းတို့၏ ကုန်ပစ္စည်းများကို လုံခုံမြှရှိစွာ ထုတ်လုပ်နိုင်ရန်အတွက်
ဤလမ်းညွှန်ပါ အကံပြုခြျက်များကို လမ်းပမြဖြေပုံသဖွယ် အသုံးပုခြန် ဝငေ့ပေးလျက်ရှိပါသည်။
မိတ်ဖက်အဖွဲ့များမှာ –

- ြစတဖြေးလျ၏ ဆိုက်ဘာလုံခုံခြေးဆိုင်ရာ စင်တာ (Australian Cyber Security Centre (ACSC))

[2] "အာဏာပိုင် အဖွေဲစီများ" ကို ဆိုလိုသည်။

- ကနဒေါ၏ ဆိုက်ဘာလုံခုံရေးဆိုင်ရာ စင်တာ (Canadian Centre for Cyber Security (CCCS))
- ယူကေနိုင်ငံများ၏ ဆိုက်ဘာလုံခုံရေးဆိုင်ရာ စင်တာ (United Kingdom's National Cyber Security Centre (NCSC–UK))
- ဂျာမနီ ဖက်ဒရယ်အစိုးရ၏ သတင်းအချက်အလက် လုံခုံရေးဆိုင်ရာ ဌာန (Germany's Federal Office for Information Security (BSI))
- နယ်သာလန်နိုင်ငံ၏ ဆိုက်ဘာလုံခုံရေးဆိုင်ရာ ဌာန (Netherlands' National Cyber Security Centre (NCSC–NL))
- နယူးဇီလန်၏ ကွန်ပျူတာဆိုင်ရာ အရေးပေါ်နှင့် တုန့်ပြန်ရေးဆိုင်ရာအသင်း (Computer Emergency Response Team New Zealand (CERT NZ)) နှင့် နယူးဇီလန်နိုင်ငံတော်၏ ဆိုက်ဘာလုံခုံရေးစင်တာ (New Zealand's National Cyber Security Centre (NCSC–NZ)) တို့ ဖစ်ပါသည်။

ပုဂ္ဂလိကကဏ္ဍမှ မိတ်ဖက်အဖွဲ့အစည်းများသည် လုံခုံမြဲရှိအောင် ပငြဆင်စီမံထားခငြးနဲ့ အလိုအလျောက် လုံခုံမြဲရှိသော ကုန်ပစ္စည်းများ ထုတ်လုပ်ရာတွင် တိုးတက်မှုရှိအောင် လုပ်ဆောင်ရာတွင် ပါဝင်ကူညီနသေည်ကို အာဏာပိုင်အဖျော်စီများမှ အသိအမှတ်ပုပြါသည်။ ၎င်းကုန်ပစ္စည်းသည် နိုင်ငံတကာ ပခြာဆိုဆွနွေးပွဲများအတွက် ဦးစားပးဆွေးနွေးစရာများအတွက် ရည်ရွယ်ပီးရင်းနှီးမြုပ်နှံရေးနှင့် အနာဂတ်တွင် လုံခုံပြီး ဘေးကင်းသည့်အပငြ် ခံနိုင်ရည်ရှိစွာ ပငြဆင်စီမံထားတဲ့ ပစ္စည်းနှင့် အလိုအလျောက်လုံခုံမြဲရှိသော ပစ္စည်းများ ထုတ်လုပ်ရာတွင် ဆုံးဖတြ်ချက်ချနိုင်ရန် ဖစြ်သည်။ အဆုံးတွင် အာဏာပိုင်အဖျော်စီများမှ ဤကုန်ပစ္စည်းနှင့်ပတ်သက်၍ သက်ဆိုင်ရာ အဖွဲ့များထံမှ ဝဖေန်အကံပြုချြက်များ ရယူပီးဘုံရည်မှန်းချက်များအောင်မငြရေးအတွက် ထပ်မံမွမ်းမံနိုင်ရန်၊ သတ်မှတ်ပငြာန်းမှုများလုပ်ရန်နှင့် ကျွန်ုပ်တို့၏ လမ်းညွှန်ချက်များကိုလည်း ထပ်ဆင့်တိုးတက်လာစရေန်အတွက် ရည်ရွယ်ပါသည်။

ကုန်ပစ္စည်းလုံခုံရေးနှင့် ပတ်သက်သည့် အရေးကီးအသေးစိတ်အချက်အလက်များ ထပ်မံသိရှိလိုပါက CISA ၏ လုံခုံမြဲမရှိတဲ့ နည်းပညာကို အသုံးပုခြငြးအတွက် ကုန်ကျစရိတ်များနဲ့ အဲဒီအတွက် ဘာတွလေုပ်ဆောင်သင့်သလဲ ဆိုသည့် ဆောင်းပါးတွင် ဖတ်ရှုနိုင်ပါသည်။

လုံခုံမြဲရှိအောင် ပငြဆင်စီမံခငြး

"လုံခုံမြဲရှိအောင် ပငြဆင်စီမံခငြး" (Secure–by–Design) ဆိုသည်မှာ မသာမာသည့် ဆိုက်ဘာတိုက်ခိုက်မှုများမှ မိမိ၏ စက်ပစ္စည်း၊ အချက်အလက်များနှင့် ဆက်သွယ်ရေးစနစ်ကို ဝင်ရောက်ကြည့်ရှုမရစရေန် အတော်အတန် ကာကွယ်မှုရှိအောင် လုပ်ဆောင်ပးထားသော စက်မှုကုန်ထုတ်

ပစ္စည်း ဖစြ်ပါသည်။ ဆော့ဖ်ဝဲပစ္စည်း ထုတ်လုပ်သူများအနဖေြ့ အရေးကီးြသည့်စနစ်များအား ဆိုက်ဘာတိုက်ခိုက်ခံရနိုင်ခြရှိမှုကို ဆန်းစစ်ဖော်ထုတ်ခငြးနှင့် မှတ်တမ်းယူခငြးများပုပြုပ်ပီး

ထိုအထဲတွင် ခတော်အလိုက်ပခြောင်းလဲဖစ်ပါ်နသေဲ ဆိုက်ဘာလုံခုံရြေး တိုက်ခိုက်မှုများအတွက် ခံရနိုင်ခရြှိသဲ ကာကွယ်မှုများ ထည့်တွက်ထားသည့် ကုန်ပစ္စည်း၏ ပုံစံပဉ် (blueprint) များကို ထည့်သွင်းသင့်ပါသည်။

အိုင်တီ (IT) နည်းပညာ၏ ဖွံ့ဖြိုးတိုးတက်မှ လုပ်ထုံးလုပ်နည်းနှင့် အလွှာအဆင့်ဆင့်ဖငြ့် နက်ရှိုင်းစွာ ကာကွယ်ထားခငြိုးဟုခ၏ါသည့် တဆင့်ခံကာကွယ်မှအလွှာများကို လုံခုံဘြားနေကင်းမှရှိအခေါ် လုပ်ဆောင်ရမည်ဖစ်ြသည်– ထိုကဲ့သို့ လုပ်ဆောင်မှသည် စနစ်များကို တိုက်ခိုက်ခံရမှမှ ကာကွယ်နိုင်ခငြိုး သို့မဟုတ် ထိလွယ်ရှလွယ်သဲ အချက်အလက်များကို တရားမဝင်နည်းဖငြ့် ရယူရန် ခက်ခဲစနေိုင်ပါသည်။ အာဏာပိုင်အဂျေင်စီများအနဖေငြ့် ကုန်ထုတ်လုပ်သူများအား အကာပြုလြှိုသည်မှာ မိမိထုတ်လုပ်သည့် ကုန်ပစ္စည်းများ ကုံရြှိနိုင်သည့် တိုက်ခိုက်မှုများကို စမ်းသပ်ရာတွင်လည်း စနစ်တစ်ခုချင်းစီအတွက် ကိုက်ညီသဲ စမ်းသပ်မှပုံစံ tailored threat model ကို အသုံးပပြီုးဖစ်ြနိုင်ခရြှိသည့် တိုက်ခိုက်မှုများအတွက် ကာကွယ်လုပ်ဆောင်ရန် အကာပြုလြှိုပါသည်။

အာဏာပိုင်အဂျေင်စီများအနဖေငြ့် ကုန်ထုတ်လုပ်သူများကို ၎င်းတို့၏ ကုန်ပစ္စည်းများနှင့် ပလက်ဖောင်းများအတွက် လုံးဝလုံခုံမြှရှိစမေည့် နည်းလမ်းကို အသုံးပုရြှေးချယ်လုပ်ဆောင်ကရြန် တိုက်တွန်းလိုပါသည်။ လုံခုံမြှရှိအခေါ် ပငြဆင်စီမံခငြိုး (secure-by-design) ထုတ်လုပ်မှတွင် ကုန်ထုတ်လုပ်မှဒီဇိုင်းအလွှာတစ်ခုခငြိုးစီအတွက် ဆောဖ့်ဝဲထုတ်လုပ်ရေးအတွက် ကြီးမြားသဲ အရင်းအမစ်ြများလိုအပ်ပီြးထုတ်လုပ်မှ ဖစ်ြစဉ်အတွင်းမှာလည်း "ထပ်မံ ဖညြ့်စွက်ရန်" ဆိုတာမျိုး မဖစ်ြစရေန်အတွက် အရင်းအမစ်ြများ လိုအပ်ပါသည်။ လုပ်ငန်းတစ်ခုအတွက် လုံခုံရြေးကို ဦးစားပးနေရော ထားရှိလုပ်ဆောင်ခငြိုးကိုလုပ်ကိုင်ရန် ထိပ်ဆုံးပိုင်းမှ ကုန်ထုတ်လုပ်သူများ၏ ခိုင်မာသည့် ခေါင်းဆောင်မှ လိုအပ်ပီြးနည်းပညာတစ်ခုတည်း ကဏ္ဍတစ်ခုတည်းမှ လုပ်ဆောင်နိုင်သည့်အရာ မဟုတ်ပါ။ ထိပ်ပိုင်းမှ စီးပွားရးေအရာရှိများနှင့် နည်းပညာအသင်းများ ပူးပေါင်းဆောင်ရွက်မှသည် သုံးစွဲသူများ၏ အသုံးချမှုမတိုင်မီနှင့် ထိန်းသိမ်းမှမှတဆင့် ဒီဇိုင်းရးဆွဲခငြိုးနှင့် ဖွံ့ဖြိုးရြှေးစတင်သည့်

အစဝေိုင်းကာလကတည်းက စတင်ဖစ်ြပါ်နရေန် လိုအပ်ပါသည်။ ကုန်ထုတ်လုပ်သူများအနဖေငြ့် သုံးစွဲသူများ "မမငြ်နိုင်သည့်အရာများ" ဖစ်ြသည့် အားနည်းချက်များပီြးခုခံနိုင်မှနည်းပါးသဲဆခေ့ဖဝဲများ ပပျောက်စရေန်အတွက် ပရိုဂမ်မင်း programming ဘာသာရပ်များ ပခြောင်းလဲအသုံးပုခြငြိုးစသည့် အတိုးအလျှော့ အပးေအယူများလုပ်ရန်နှင့် ရင်းနှီးမြပြိုနှံမှုများ လုပ်ကရြန် တိုက်တွန်းလိုပါသည်။ ၎င်းတို့အနဖေငြ့် ဆွဲဆောင်မှရှိသော်လည်း တိုက်ခိုက်မှ မျက်နှာပငြ်ဖစ်ြစနိုင်သည့် ကုန်ပစ္စည်း၏ သွင်ပငြ်အင်္ဂါများကို ဦးစားပးေမည့်အစား သုံးစွဲသူများကို ကာကွယ်ပးေမည့် အရာများကို အသုံးပမြည့် စက်ယန္တရားများကို ဦးစားပးေသင့်ပါသည်။

အားနည်းချက်ရှိနသေည့် စက်မှကို မသမာသည့် ဆိုက်ဘာတိုက်ခိုင်မှများ ရပ်တန့်အခေါ် လုပ်ဆောင်ရာတွင် ဖခြရှင်းချက် တစ်ခုတည်း မရှိပါ။ လုံခုံမြှရှိအခေါ် ပငြဆင်စီမံထားသည့် (secure-by-design) ကုန်ပစ္စည်းများသည် အားနည်းချက်အပ၏ါမူတည်ပီြးဆက်လက် တိုက်ခိုက်ခံရမည် ဖစ်ြသော်လည်း ထိုအားနည်းချက် အများစုသည် သေးငယ်သဲ ပဩနာအရင်းအမစ်ြမှ ဖစ်ြပ၏ါလာခငြိုး ဖစ်ြပါသည်။ ကုန်ထုတ်လုပ်သူများအနဖေငြ့် လက်ရှိကုန်ပစ္စည်းများကို လုံခုံစွာပငြ်ဆင်စီမံခငြိုး နည်းလမ်းများနှင့် ချိန်ညိရန်

ရေးသားထားသလေလမ်းပမြဲြပုံများကို ဖော်ဆောင်ပေးသင့်ပြီးထူးခြားသည့်အခြေအနများတွင်သာ သွဖြီသွားရန်ဆောင်ရွက်သင့်သည်။

သုံးစွဲသူများအတွက် လုံခုံရြေးရလာဒ်နှင့် အဆင့်မငြ့် လုံခုံရြေးလုပ်ဆောင်မှုသည် ကုန်ထုတ်လုပ်မှ စရိတ်ပိုများပြားလာနိုင်သည်ကို အာဏာပိုင် အကျေငစ်ီများ နားလည်ပါသည်။ သို့သော်လည်း လုံခုံမြှရှိအောင် ပငြ်ဆင်စီမံထားသည့် စက်မှုများကို ထုတ်လုပ်ရန်အတွက် ရင်းနှီးမြုပြန်ုပီးြတဖက်တွင်လည်း ကုန်အသစ်များ ထုတ်လုပ်နရေင်း လက်ရှိ ကုန်များကိုလည်း ရရှေည်ထိန်းသိမ်းနိုင်မှလုပ်နိုင်ခငြ်းသည် သုံးစွဲသူများအတွက် လုံခုံရြေးနှင့် အချက်အလက်အခိုးခံရမှုမျိုးမဖစ်ြအောင် ပိုမိုကာကွယ်ပေးရာရောက်နိုင်ပါသည်။ လုံခုံမြှရှိအောင် ပငြ်ဆင်စီမံခငြ်း အခြေခံမူသည် သုံးစွဲသူများအတွက် လုံခုံမြှပေးပီြး ကုန်ထုတ်လုပ်သူ၏ အမှတ်တံဆိပ်ဂုဏ်သတင်းကို ကျော်စောစေရုံသာမက ရရှေည်တွင် ကုန်ထုတ်လုပ်သူတွအေတွက် ပူပြငြ်ထိန်းသိမ်းမှနှင့် ဖာထေးမှအတွက် ကုန်ကျစရိတ်ကိုလည်း လျော့နည်းစနိုင်ပါသည်။

အောက်ပါအချက်အလက်များသည် ဆော့ဖ်ဝဲထုတ်လုပ်သူများအတွက် အကံုပြုချက်များ၏ စာရင်းဖစ်ြပီးြ ကုန်ထုတ်လုပ်ရာတွင် ထည့်သွင်းစဉ်းစား အသုံးပုနှိုင်သည့် လုပ်ထုံးလုပ်နည်းများနှင့် မူဝါဒများကို အကံုပြုြထားခငြ်း ဖစ်ြပါသည်။

လုံခုံမြှရှိအောင် ပငြ်ဆင်စီမံခငြ်း

“Secure-by-Default” အလိုအလျောက် လုံခုံမြှရှိနခေငြ်း ဆိုသည်မှာ ငွကေငြးထပ်မံ ကုန်ကျခံစရာမလိုဘဲ တိုက်ခိုက်ခံရမှုနည်းလမ်းများကို ခံနိုင်ရည်ရှိရန်အတွက် တည်ဆောက်ထားသည့် ကုန်ပစ္စည်းများကို ဆိုလိုပါသည်။ ထိုပစ္စည်းများသည် ကျယ်ကျယ်ပန့်ပန့်ဖစ်ြပါေါ်နသေော ခိမြိုးခြောက်မှုများနှင့် အားနည်းချက်များကို ကာကွယ်ပေးခငြ်းဖစ်ြပီးြထိုကဲ့သို့ အကာအကွယ်ရရှိရန်အတွက် ဝယ်ယူသုံးစွဲသူများမှ ပိုမိုကုန်ကျခံစရာမလိုခငြ်းမျိုး ဖစ်ြပါသည်။ Secure-by-default အလိုအလျောက် လုံခုံမြှရှိနသေည့် ကုန်ပစ္စည်းကို သုံးစွဲသူများအသုံးပုသြည့်အခါ အလိုအလျောက် လုံခုံနြခေငြ်းရှိသည့်နည်းလမ်းမှ သွဖြီသည့်အခါတွင် အချက်အလက်ချိုးဖောက်ခံရမှုများ ခံရနိုင်ခြေများကြောင်း သချောသိနားလည်အောင် လုပ်ဆောင်ထားရန်လိုအပ်ပီးြတခြနည်းလမ်းဖငြ့် ကာကွယ်ပေးမည့် နောက်ထပ်ထိန်းချုပ်မှုများ ထပ်ရယူမှသာ ရနိုင်မည့်အကြောင်းပါ သိထားအောင် လုပ်ရန်လိုအပ်ပါသည်။

- လုံခုံမြှရှိသည့် ဖွံ့စည်းပုံစနစ်သည် အခြေခံဖစ်ြသင့်ပါသည်။ အလိုအလျောက် လုံခုံနြသော ပစ္စည်း (Secure-by-Default products) သည် မသမာသော ဆိုက်ဘာတိုက်ခိုက်မှုများကို အကာအကွယ်ပေးနိုင်ရန်အတွက် လိုအပ်သော ထိန်းချုပ်မှုများကို အလိုအလျောက်ပေးထားသည့်အပငြ် ထပ်မံကုန်ကျရန် မလိုအပ်ဘဲ လုံခုံရြေးဆိုင်ရာ အစိတ်အပိုင်းကို အသုံးပုခြင့် ပေးထားပါသည်။
- လုံခုံရြေးဆိုင်ရာ တည်ဆောက်ပုံ၏ ရုပ်ထွေးမှုသည် သုံးစွဲသူများအတွက် ပဿနာမဖစ်ြသင့်ပ။ အိုင်တီ အဖွဲ့အစည်းမှ အမူထမ်းများအနနှေင့် လုံခုံရြေးဆိုင်ရာနှင့် လုပ်ငန်းလည်ပတ်ခငြ်းဆိုင်ရာ

တာဝန်များဖြင့် ဝန်ပိနလေ့ရှိသည်။ ထိုကြောင့် လုံခုံရေးပဏာမနာနှင့် ခိုင်ခံ့ပြည့်စုံသော လုံခုံရေးစနစ်ရရှိခြင်းကို နားလည်သဘောပေါက်အောင် လုပ်ဆောင်ရာတွင် အကန့်အသတ်ရှိနိုင်ပါသည်။ လုံခုံရေးဆိုင်ရာ တည်ဆောက်ပုံအား တိုးမြှင့်လုပ်ဆောင်ခြင်းအားဖြင့် – အလိုအလျောက်လမ်းကြောင်းများ ပွင့်စေခြင်းအားဖြင့် – ကုန်ထုတ်လုပ်သူများသည် ၎င်းတို့၏ ဝယ်ယူသုံးစွဲသူများလိုအပ်သည့် ပစ္စည်းများ ထုတ်လုပ်နိုင်ရန်၊ ဖန်ဖြူးရှင်းလုပ်ဆောင်ရာတွင် အလိုအလျောက် လုံခုံခြင်သော အဆင့်သတ်မှတ်ချက်နှင့်အညီ လုပ်ဆောင်ထားပေးနိုင်ပါသည်။

အလိုအလျောက် လုံခုံမြှင့်ရှိသော ကုန်ပစ္စည်းဆိုသည်မှာ ပိုမိုလုံခုံမြှင့်ရှိအောင်လုပ်ဆောင်ထားပြီး ထိုမွမ်းမံမှုအတွက် ပိုမို တာဝင်းခံမှုများ မလုပ်ထားပါ။ ၎င်းအစား ကားအသစ်တွင် ထိုင်ခုံခါးပတ် (seatbelt) လို အခြေခံကုန်အနဖြင့် အလိုအလျောက် ပါလာပြီးသားဖစ်အောင် ထည့်သွင်းလိုက်တာမျိုး ဖစ်ပါသည်။ လုံခုံရေးသည် ဇိမ်ခံရန် မဟုတ်သည့်အတွက် ထိုလုံခုံရေးအတွက် သုံးစွဲသူများမှ အပေးအယူလုပ်စရာမလိုအောင် သို့မဟုတ် အဖိုးအခ ထပ်မံပေးစရာမလိုဘဲ လူတိုင်းရသင့်သည့် အနအေထားဖစ်အောင် လုပ်ဆောင်ရမည်ဖစ်ပါသည်။

ဆော့ဖ်ဝဲကုန်ထုတ်လုပ်သူများအတွက် အကံပြုချက်များ

ဤအာဏာပိုင်အဂျေင်စီများ၏ ပူးတွဲအကံပြေးချက်များသည် ကုန်ထုတ်လုပ်သူများအနဖြင့် အိုင်တီလုံခုံရေးရှိစရေန်နှင့် လုံခုံရေးအစီအစဉ်များ အကောင်အထည်ဖော်ရာတွင် လမ်းညွှန်ချက်ရေးဆွဲရန်အတွက် အကံပြုချက်များ ဖစ်ပါသည်။ အာဏာပိုင်အဂျေင်စီများအနဖြင့် ဆော့ဖ်ဝဲကုန်ထုတ်လုပ်သူများအား အောက်ပါ ဗျူဟာအတိုင်း အကောင်အထည်ဖော်ကရှိန် အကံပြုထိုပီး လုံခုံမြှင့်ရှိအောင် ပဉ်ဆင်စီမံထားခြင်းနှင့် အလိုအလျောက်လုံခုံမြှင့်ရှိနခြေင်း အခြေခံမူမှတဆင့် ၎င်းတို့၏ သုံးစွဲသူများ လုံခုံရေးရလာဒ် ရရှိစရေန် ဦးဆောင်ဦးရွက်ပုရှိန် အကံပြုပါသည်။

ဆော့ဖ်ဝဲကုန်ပစ္စည်းများအတွက် လုံခုံရေးဆိုင်ရာ အခြေခံမူများ

စက်မှုကုန်ပစ္စည်းထုတ်လုပ်သူများအနဖြင့် ဆော့ဖ်ဝဲလုံခုံရေးကို ဦးစားပေး အာရုံစိုက်ထားသည့် ဗျူဟာအား လက်စွဲအနဖြင့် အသုံးပုရှိန် တိုက်တွန်းလိုပါသည်။ အာဏာပိုင်အဂျေင်စီများသည် ဆော့ဖ်ဝဲကုန်ထုတ်လုပ်သူများအနဖြင့် ၎င်းတို့၏ ဆော့ဖ်ဝဲကို မထုတ်လုပ်မီ၊ အခြေပစ္စည်းနှင့် တွဲဖက်သုံးစွဲမှုမပုခြင်နှင့် ကုန်ပစ္စည်း တင်ပို့မှုမလုပ်မီ ဆော့ဖ်ဝဲဒီဇိုင်းရေးဆွဲနသည့်အဆင့်တွင် အောက်ပါ အဓိက အခြေခံမူ ၃ ချက်ကို လမ်းညွှန်အဖစ် အသုံးပုနှိုင်ရန်အတွက် ရေးဆွဲပေးထားပါသည်။

1. လုံခုံရေးဝန်ကို သုံးစွဲသူများအပေါ်သာ ကျခံစတောမျိုးမဖစ်သင့်ပါ။
   ဆော့ဖ်ဝဲကုန်ထုတ်လုပ်သူများအနဖြင့် လုံခုံရေးတာဝန်ကို ယူပြီးသုံးစွဲသူများအတွက် လုပ်ဆောင်ပေးရမည်ဖစ်ပြီးခတော်နှင့်အညီ မိမိ၏ ကုန်ပစ္စည်းကို လိုက်လံပခြောင်းလဲရမည် ဖစ်သည်။

2. ကြီးမားသိသာသည့် ပွင့်လင်းမြင်သာမှုရှိခြင်းနှင့် တာဝန်ခံမှုများကို လက်ခံကျင့်သုံးပါ။ ဆော့ဖ်ဝဲထုတ်လုပ်သူများအနေဖြင့် လုံခြုံပြီး၊ ဘေးကင်းသည့် ကုန်ပစ္စည်းများ ထုတ်လုပ်နိုင်မှုအပေါ် ဂုဏ်ယူဝင့်ကြွားသင့်သည့်အပြင် ကုန်ထုတ်လုပ်သူ အသိုင်းအဝိုင်းအတွင်း အခြားသူများနှင့်မတူအောင် လုပ်ဆောင်ပေးနိုင်သည့်အတွက် တမူထူးခြားမည်ဖြစ်ပါသည်။ ထိုအထဲမှာ ခိုင်မာစစ်မှန်သည့် နည်းပညာယန္တရား သုံးစွဲမှု အလိုအလျောက်များလာခြင်း စသည့် သုံးစွဲသူများ၏ ထိရောက်စွာ အသုံးချနိုင်မှုမျိုးကို သိရှိရသည့်အခါ ထိုအချက်အလက်များကို မျှဝေခြင်းမျိုး ဖြစ်ပါသည်။ အားနည်းချက်များကို ဖော်ပြခြင်း (vulnerability advisories) နှင့် ပူးတွဲဖြစ်တတ်သည့် အားနည်းချက်များနှင့် ဖော်ထုတ်သည့် (common vulnerability and exposure (CVE)) မှတ်တမ်းများကို ဖြည့်စွက်ပြီး၊ မှန်ကန်စွာ လုပ်ထားခြင်းသည်လည်း အရေးကြီးသည့်လုပ်ဆောင်ချက် ဖြစ်ပါသည်။ သို့သော် ထို CVE မှတ်တမ်းအချက်အလက်ထုတ်ဖော်မှုအား အဆိုးဖက်ဆောင်သည့် အနေအထားအဖြစ် မမြင်နိုင်ခြင်းကို သတိထားသင့်ပါသည်၊ ထိုအချက်အလက်များသည် ကုန်ပစ္စည်း၏ အရည်အသွေးကို ရှာဖွေ ဆန်းစစ်စမ်းသပ်မှု (healthy code analysis) နှင့် ဆော့ဖ်ဝဲများကို စမ်းသပ်ပေးသည့် အသိုင်းအဝိုင်း (testing community) ရှိခြင်း ၏ လက္ခဏာကောင်းများ ဖြစ်သည်ကို ရည်ညွှန်းပေးသော မှတ်တမ်းဖြစ်ပါသည်။

3. ထိုရည်မှန်းချက်များ အောင်မြင်ရန်အတွက် ဖွဲ့စည်းပုံရေးဆွဲတည်ထောင်ခြင်းနှင့် ခေါင်းဆောင်ပိုင်းဆိုင်ရာ ဦးဆောင်မှုများရှိအောင် တည်ဆောက်ရပါမည်။ စက်မှုကုန်ပစ္စည်းများ ထုတ်လုပ်ရာတွင် စက်မှုကျွမ်းကျင်မှုများရှိရန် အရေးကြီးသကဲ့သို့ အဖွဲ့အစည်းအတွင်း ဖြစ်ပေါ်သည့် အပြောင်းအလဲများကို အကောင်အထည်ဖော်ဆောင်ရာတွင် အဓိက ဆုံးဖြတ်ချက်ပေးသူများမှာ ထိပ်ပိုင်းမှ အရာရှိများ ဖြစ်ကြပါသည်။ ဆော့ဖ်ဝဲကုန်ထုတ်လုပ်ငန်းတွင် လုံခြုံဘေးကင်းရေးကို ဦးစားပေးလုပ်ရမည်ဟု ထိပ်သီး အလုပ်အမှုဆောင်အဆင့်မှ သတ်မှတ်ထားလျှင် ထိုအချက်ကို သုံးစွဲသူများ၏ နားလည်မှုရရှိရန် လိုအပ်ပါသည်။

   a. ထုတ်လုပ်သည့်ကုန်များသည် တိုက်ခိုက်မှုများကို ခံနိုင်ရည်ရှိမရှိ စမ်းသပ်ရာတွင်လည်း တစ်ခုခြင်းစီအတွက် ကိုက်ညီတဲ့ပုံစံမျိုး tailored threat model နှင့် စမ်းသပ်ရန်လိုသကဲ့သို့ ကုန်ပစ္စည်းကို ထိရောက်စွာအသုံးပြုနိုင်ရေးအတွက် လမ်းညွှန်ချက်တွထောရှိရန်

   b. အလိုအလျောက် လုံခြုံမှုရှိနေခြင်း အခြေခံမှုနှင့် ကိုက်ညီနေရန် လုံခြုံရေးထိန်းချုပ်မှုဆိုင်ရာ ကမ်းလှမ်းချက်ကို အကောင်အထည်ဖော်ရန်

   c. ကုမ္ပဏီ၏ အရွယ်အစားအပေါ် မူတည်၍ ကိုက်ညီမည့် အရင်းအမြစ်ကိုလည်း ဖျှဟာကျကျ ထားရှိရန်နှင့် လုံခြုံမှုရှိအောင် ပြင်ဆင်စီမံခြင်းအလေ့အထနှင့် ကိုက်ညီရန်အတွက် ထုတ်လုပ်မှုဆိုင်ရာ လုပ်ထုံးလုပ်နည်းကို ထားရှိရန်

   d. လုံခြုံရေးဆိုင်ရာ ကိစ္စနှင့်ပတ်သက်၍ အတွင်း အပြင် (ဥပမာ အမှုထမ်းနှင့် သုံးစွဲသူများ၏ ဝဖေန်အကံပြုချက်များ) ၏ ဝဖေန်အကံပြုချက်များအတွက်

တံခါးဖွင့်လှစ်ထားရန်လိုအပ်ပါသည်။ ဆဋ္ဌဖဝဲလုံခုံရြေးသည် အလုပ်တွင်းဖိုရမ် (ဥပမာ အခမ်းအနားတစ်ရပ်အနဖေငြ့် အားလုံးပါဝင်သဘော ဆွေးနွေးမှု သို့မဟုတ် ခတ္တာတနားနချေိန်အတွင်း ဆွေးနွေးပြောဆိုမှု) များကို အလေးထားသင့်သည့်အပငြ် အပငြ်ပိုင်းထုတ်ကုန် စျေးကွက်မငြ့်တင်ရေးနှင့် သုံးစွဲသူများနှင့် ချိတ်ဆက်မှသည်လည်း အရေးပါပါသည်။

e. သုံးစွဲသူများအတွက် ကာင်းမွန်စွာ အသုံးဝင်မှုကို တိုင်းတာရန် လိုအပ်ပါသည်။ ထိပ်သီးခေါင်းဆောင်များအနဖေငြ့် လုံခုံအြောင် ပငြ်ဆင်စီမံခငြ်းနှင့် အလိုအလျောက် လုံခြုံသည့်အနအေထားဖစြ်အောင်လုပ်ဆောင်ခငြ်းအားဖငြ့် သုံးစွဲသူများအား မည်သည့်နရောတွင် အကျိုးပြုနကေြာင်းနှင့် ဖာထေးရခငြ်းများ၊ အမှားပငြ်ဆင်ချက်နည်းပါးခငြ်းနှင့် တိုက်ခိုက်ခံရမှု နည်းပါးသည့် အကြောင်းများကို ကြးလိုကမြည်ဖစြ်ပါသည်။

ထိုအခငြခံမှ ၃ ချက်ကို အသုံးပုငြ်ရန်အတွက် ကုန်ထုတ်လုပ်သူများအနဖေငြ့် ၎င်းတို့၏ ကုန်ထုတ်လုပ်မှ လုပ်ငန်းစဉ်တွင် လည်ပတ်ခငြ်းဆိုင်ရာ ဗျူဟာတချို့ကို ထည့်သွင်းစဉ်းစားသင့်ပါသည်။

အဖွဲ့အစည်းအတွင်း လုံခုံမြှရှိအောင် ပငြ်ဆင်စီမံထားခငြ်းနှင့် အလိုအလျောက် လုံခုံမြှရှိနခေငြ်းနည်းလမ်းများ အရေးပါမှုကို ဖော်ဆောင်ရန်အတွက် ကုမ္ပဏီထိပ်သီးခေါင်းဆောင်များနှင့် ပုံမှန်အစည်းအဝေးများ ကျင်းပရန်လည်း အရေးကီးပါသည်။ အခငြခံမှများအတိုင်း လိုက်နာထုတ်လုပ်သည့် အသင်းများကို ဂုဏ်ပုငြ်ပီးငြ ထိုအထဲတွင်း ဆဋ္ဌဖဝဲလုံခုံမြှရှိအောင် ထူးခငြားစွာ စွမ်းဆောင်အကောင်အထည်ဖော်နိုင်မှအတွက် ဆုချီးမငြ့်ခငြ်း သို့မဟုတ် ရာထူးတိုးမငြ့်ပနေခငြ်းများ လုပ်ဆောင်နိုင်ရန်အတွက် မူဝါဒနှင့် လုပ်ထုံးလုပ်နည်းများ ချမှတ်ထားရန်လည်း လိုအပ်ပါသည်။

ဆဋ္ဌဖဝဲလုံခုံမြှအား အရေးထားခငြ်းသည် လုပ်ငန်းအောင်မငြ်ခငြ်းဟူသည့် ဆောင်ပုဒ်ဖငြ့် လုပ်ငန်းကို လည်ပတ်သင့်ပါသည်။ ဥပမာ "ဆဋ္ဌဖဝဲလုံခုံရြေး ခေါင်းဆောင်" တစ်ဦး သို့မဟုတ် "ဆဋ္ဌဖဝဲလုံခုံရြေးအဖွဲ့" တစ်ဖွဲ့ကို စီးပွားရေးလုပ်ငန်းနှင့် အိုင်တီလုပ်ထုံးလုပ်နည်းများကို ဆဋ္ဌဖဝဲလုံခုံရြေးစံနှုန်းများနှင့် တာဝန်ခံယူမှုရှိသဘော ကုန်ထုတ်လုပ်မှုနှင့် တိုက်ရိုက်ချိတ်ဆက်ရန် ခန့်အပ်ခငြ်းကို စဉ်းစားပါ။ ကုန်ထုတ်လုပ်သူများအနဖေငြ့် ၎င်းတို့တွင် ခိုင်ခံ့ လွတ်လပ်သည့် လုံခုံရြေးဆန်းစစ်မှုရှိခငြ်းနှင့် ၎င်းတို့၏ ထုတ်ကုန်များကို ပန်ြလည်ဆန်းစစ်ပေးသည့် အစီအစဉ်များ ချထားရန် လိုအပ်ပါသည်။

ကုန်ထုတ်လုပ်သည့်ကာလတွင် အရေးအကြီးဆုံးနှင့် သက်ရောက်မှုအများဆုံးဖစ်သော ကုန်များကို ဦးစားပေးထုတ်လုပ်နိုင်ရန်အတွက် ကုန်ပစ္စည်း၏ လုံခြုံရေးဆိုင်ရာ တိုက်ခိုက်နိုင်ခြေရှိမှုများအား စမ်းသပ်ရာတွင်လည်း တစ်ခုခြင်းစီအတွက် ကိုက်ညီသော စမ်းသပ်မှုပုံစံအတိုင်း လုပ်ဆောင်သင့်ပါတယ်။ တိုက်ခိုက်နိုင်ခြေရှိမှုများအား စမ်းသပ်ခြင်းသည် ကုန်ပစ္စည်း၏ အဓိက အသုံးပြုမှုကို ထည့်သွင်းစဉ်းစားမှုဖစ်စေသည့်အပြင် ကုန်ထုတ်လုပ်သည့်အသင်းသားများအားလည်း ကုန်ပစ္စည်းကို ပိုကောင်းမွန်စေရန် အားဖြည့်လုပ်ဆောင်စေနိုင်ပါသည်။ နောက်ဆုံးတွင် ထိပ်သီးခေါင်းဆောင်များအနေဖြင့် လုံခြုံမြဲရှိသည့်ကုန်ပစ္စည်းများကို အကောင်းဆုံးနှင့် အရည်အသွေးအမင့်ဆုံး ထုတ်လုပ်ရန်အတွက် ကုန်ပစ္စည်းထုတ်လုပ်သည့် အသင်းများကို တာဝန်ယူမှု တာဝန်ခံမှုရှိအောင် လုပ်ထားသင့်ပါသည်။

လုံခြုံမြဲရှိအောင် ပြင်ဆင်စီမံခြင်း၏ ဗျူဟာများ

လုံခြုံဘေဆဲ့ဖ်ဝဲထုတ်လုပ်ရေးမူဘောင် (Secure Software Development Framework (SSDF)) သို့မဟုတ် စံနှုန်းများနှင့် နည်းပညာဆိုင်ရာ အမျိုးသားသိပ္ပံပံ (National Institute of Standards and Technology's (NIST)) SP 800–218 ဟုလည်း သိကြသည့်အရာသည် လုံခြုံရေးအဆင့်မြင့်သော ဆဲ့ဖ်ဝဲကုန်ထုတ်လုပ်မှု၏ လုပ်ထုံးလုပ်နည်းအစုဖစ်ပြီးကြထိုအရာကို ဆဲ့ဖ်ဝဲကုန်ထုတ်လုပ်မှု အဆင့်ဆင့်၏ သက်တမ်းတွင် (SDLC) ထည့်သွင်းအသုံးပြုနိုင်ပါသည်။ ထိုကဲ့သို့ လုပ်ထုံးလုပ်နည်းများကို လုပ်ခြင်းအားဖြင့် ဆဲ့ဖ်ဝဲကုန်ထုတ်လုပ်သူများအား ဆဲ့ဖ်ဝဲထုတ်လုပ်ရာတွင် အားနည်းချက်များကို ပိုမိုရှာဖွေတွေ့ရှိကာ ဖယ်ရှားနိုင်စေကဲ့သို့ အားနည်းချက်များကြောင့် ဖစ်ပေါ်လာတတ်သည့် ဆိုးကျိုးများကိုလည်း လျော့ပါးစေနိုင်သည့်အပြင် ထိုအားနည်းချက်များအား ဖစ်စေသည့်အကြောင်းရင်းများကို သိရှိနိုင်ပြီး အနာဂတ်တွင် ထပ်မဖစ်ရန် ကာကွယ်လုပ်ဆောင်စေနိုင်မည်ဖစ်ပါသည်။

အာဏာပိုင် အဖျော်စီများအနေဖြင့် လုံခြုံမြဲရှိအောင် ပြင်ဆင်စီမံသော ဗျူဟာအား အသုံးပြုရန် တိုက်တွန်းလိုပါကြထိုအထဲတွင် SSDF ၏ လုပ်ထုံးလုပ်နည်းများကို အခြေခံသည့်မူများအား အသုံးပြုခြင်းလည်း ပါဝင်ပါသည်။ ဆဲ့ဖ်ဝဲ ထုတ်လုပ်သူများအနေဖြင့် ၎င်းတို့၏ ကုန်ပစ္စည်းများကို ထုတ်လုပ်ရာတွင် လုံခြုံမြဲရှိအောင် ပြင်ဆင်စီမံသော ဗျူဟာအား ပိုမိုအသုံးပြုရန် လမ်းပြမြေပုံကို အသုံးပြု၍ ထုတ်လုပ်သင့်ပါသည်။ အောက်ပါအချက်များသည် ပြည့်စုံစွာပမ်မှမရှိသော်လည်း လမ်းပြမြေပုံရေးဆွဲရာတွင် ပုံဖော်နိုင်ရန် အထောက်အကူပုံစြနိုင်သည့် လုပ်ထုံးလုပ်နည်းများ ဖစ်ပါသည်။

- ကွန်ပျူတာ memory လုံခြုံရေးအတွက် ကောင်းမွန်သော ဘာသာရပ်များ Memory safe programming languages (SSDF PW.6.1) – အခွင့်သာတိုင်း memory လုံခြုံရေးအတွက် ကောင်းမွန်သော ဘာသာရပ်များကို (memory safe languages) ဦးစားပေးအသုံးပြုပါ။ အာဏာပိုင်အဖျော်စီများအနေဖြင့် အခြားသော ကွန်ပျူတာမှတ်ဥာဏ်ကို ကာကွယ်သော နည်းလမ်းဖစ်သည့် address space layout randomization (ASLR), control–flow integrity

(CFI) နှင့် fuzzing တို့သည် legacy codebase များအတွက် အသုံးပုံနိုင်ကြောင်းကို နားလည်ပါသည်။ သို့သော် ၎င်းသည် လုံခုံမြဲရှိအောင် ပင်ငြိဆင်စီမံထားခြင်းဟု ဆိုလိုရန် မလုံလောက်သေးပါ အဘယ်ကြောင့်ဆိုသော် ၎င်းတို့သည် အားနည်းချက်အပေါ် တိုက်ခိုက်မှုဒဏ်ကို ကာကွယ်နိုင်သည့်အတွက် ဖြစ်ပါသည်။ ခေတ်ပေါ် memory လုံခုံရေး ဘာသာရပ် (Modern memory safe language) ၏ ဥပမာ တချို့မှာ C#, Rust, Ruby, Java, Go နှင့် Swift တို့ ပါဝင်ပါသည်။ NSA ၏ memory လုံခုံရေးအကြောင်း ပိုမို သိရှိလိုပါက ဤအချက်အလက်လွှာ တွင် လေ့လာနိုင်ပါသည်။

- လုံခုံသြော ဟဒ်ဝဲအခြေခံအုတ်မြစ် (Secure Hardware Foundation) – ဆော့ဖ်ဝဲရေးရာတွင် အသေးစိတ် memory ကာကွယ်ခြင်းနည်းကို ထည့်သွင်းအသုံးပုံပြု၊ ဥပမာ Capability Hardware Enhance RISC Instructions (CHERI) ကန ဖော်ပြထားတာမျိုးဖစ်ပြီး သမားရိုးကျ ဟဒ်ဝဲများကို ဆက်နွယ်အသုံးပုံနိုင်စသော့ အရာများဖစ်သည့် Instruction–Set Architectures (ISAs) တို့ ဖစ်ပါသည်။ အချက်အလက်များ ပိုသိလိုပါက Cambridge တက္ကသိုလ်၏ CHERI ဝဘ်ဆိုက်စာမျက်နှာ တွင် လေ့လာနိုင်ပါသည်။
- လုံခုံမြဲရှိသော ဆော့ဖ်ဝဲအစိတ်အပိုင်းများ (Secure Software Components) (SSDF PW 4.1) – စော့စပ်သခြေပြီး လုံခုံမြဲရှိသည့် ဆော့ဖ်ဝဲအစိတ်အပိုင်းများကို ဝယ်ယူသုံးစွဲပါ။ (ဥပမာ software libraries, modules, middleware, frameworks) ကို လိုင်စင်ရကုမ္ပဏီများ၊ လူတိုင်းထည့်ဝင်နိုင်သည့် open source နှင့် အခြား တတိယ ပါတီထုတ်လုပ်သူများထံမှ ရယူထိန်းသိမ်းပါ။
- ဝက်ဆိုက်စာမျက်နှာပုံစံပြားဆိုင်ရာ မူဘောင်များ (Web template frameworks) (SSDF PW.5.1) – Cross–site scripting ကဲ့သို့သော user input တိုက်ခိုက်မှုကို အလိုအလျောက် ရှောင်ရှားနိုင်သည့် web template framework များကို အသုံးပုံပြု။
- Parameterized queries (SSDF PW 5.1) – SQL injection တိုက်ခိုက်မှုကို ရှောင်ရှားရန်အတွက် queries ထဲတွင် user input ပါဝင်နသော်ကို အသုံးပုမြည့်အစား parameterized queries ကို အသုံးပုံပြု။
- ပုံသနှင့် ပြောင်းလဲမှုရှိသောအပ်ပလီကေးရှင်း လုံခုံရေး စမ်းသပ်မှ (Static and dynamic application security testing) (SAST/DAST) (SSDF PW.7.2, PW.8.2) – ပုံသနှင့် ပြောင်းလဲမှုရှိသော လုံခုံရေး စမ်းသပ်မှ (SAST/DAST) ကို အသုံးပု၍ ဆော့ဖ်ဝဲ၏ အရင်းအမစ်ကုဒ်ကို ဆန်းစစ်ပီး ဖစ်တတ်သည့် အမှားများ၏ အမူအကျင့်များကို ဖော်ထုတ်နိုင်ရန် အသုံးပုံပြု။ ၎င်းတို့သည် ဆော့ဖ်ဝဲတွင် ဖစ်တတ်သည့် memory ပဿနာမှ သိလှောင်ထားသည့် အချက်အလက်များရယူရာတွင် ဖစ်တတ်သည့်အမှားများအတွက် အကျုံးဝင်စသော့ (ဥပမာ – SQL injection ကို မကာကွယ်သည့် အချက်အလက်ထည့်သွင်းမှု) တို့ ဖစ်ပါသည်။ SAST နှင့် DAST တို့သည် အခြားသော စမ်းသပ်မှုများနှင့် လိုက်လျောညီထွေ ကိုက်ညီမှု ရှိသင့်ပါသည်။ မျှော်မှန်းထားသည့် လုံခုံရေးရရှိရန်အတွက် ထိုဆော့ဖ်ဝဲသည် တစ်ခုချင်းစီအတွက် စမ်းသပ်သည့်အခါတွင်ဖစ်စေ

ပခေါင်းစပ်ထားသည့်အရာအတွက်ဖစ်စေ ကိုက်ညီမှု ရှိသင့်ပါသည်။ ပဩဿနာကို သိရသည့်အခါ ထုတ်လုပ်သူများအနေဖြင့် အားနည်းချက်ဖစ်စေသည့် အရင်းအမစ်ကို စနစ်တကျ ဖော်ထုတ်ဆန်းစစ်မှု လုပ်သင့်ပါသည်။

- ကုဒ်သုံးသပ်ချက် (Code review) (SSDF PW.7.1, PW.7.2) – အရည်အသွေးမြင့်သော ဆော့ဖ်ဝဲဖစ်ရန်အတွက် ထည့်သွင်းထားသည့် ကုဒ်များကို အခြား ဆော့ဖ်ဝဲရေးသူနှင့် လုပ်ဖော်ကိုင်ဖက်များ၏ ဆန်းစစ်မှု မှတ်ချက်များ ရယူရန် ကိုးစားသင့်ပါသည်။
- Software Bill of Materials (SBOM) (SBOM) (SSDF PS.3.2, PW.4.1) – အခြားသော ဆော့ဖ်ဝဲများပါဝင်ပါက တီထွင်မှုတွင် SBOM[3] ကို ထင်သာမြင်သာမှုရှိရန် လုပ်ဆောင်ပီးမြှ ထည့်သွင်းအသုံးပုဩင့်ပါသည်။
- အားနည်းချက်ဖော်ပဩသည့် အစီအစဉ်များ (Vulnerability disclosure programs) (SSDF RV.1.3) – လုံခုံရေး သုတသေများ တွေ့ရှိသည့် အားနည်းချက်များကို ဖော်ပစြနိုင်မည့် အစီအစဉ်များ ချမှတ်တည်ထောင်ထားသင့်ပီး အားနည်းချက်များကို ထုတ်ဖော်ပခြောဆိုသည့်အခါတွင်လည်း တရားရေးရာအရ ကာကွယ်မှုရှိအောင် လုပ်ဆောင်ပေးရပါမည်။ ဤအစီတ်အပိုင်းတစ်ခုအဖစ် ထုတ်လုပ်သူများသည် အားနည်းချက်များ၏ အရင်းအမစ်ကို ရှာဖွေဖော်ထုတ်နိုင်မည့် လုပ်ငန်းစဉ်ကိုလည်း ချမှတ်ထားရှိသင့်ပါသည်။ ထိုလုပ်ငန်းစဉ်ထဲတွင် လုံခုံခြောင် ပင်ဆင်စီမံခဲ့ပီး လုပ်ထုံးလုပ်နည်း (သို့မဟုတ် အခြား ဆင်တူမှုရှိသော လုပ်ထုံးလုပ်နည်းများ) ကို အသုံးပုခြင်းသည် အားနည်းချက်ဖစ်ပါ်တတ်သည်ကို ကာကွယ်ပေးနိုင်ခဲ့ပီး ရှိမရှိဆိုသည့်အချက်ကိုပါ ထည့်သွင်းစဉ်းစားသင့်ပါသည်။
- CVE ပည့်စုံခဲ့ပီး (CVE completeness) – ဆော့ဖ်ဝဲထုတ်လုပ်မှု ကဏ္ဍကတစ်ခုလုံးအတွက် လုံခုံရေး အားနည်းချက်ဖစ်စေသည့် ပဩဿနာအရင်းအမစ်ကို စိစစ်စိတ်ဖခြဆန်းစစ်မှု လုပ်ဆောင်ရာတွင် ထုတ်ဝေထားသည့် CVE မှတ်တမ်းများတွင် ပဩဿနာဖစ်စေသည့် အရင်းအမစ်အချက်အလက်များ သို့မဟုတ် ဖစ်တတ်သည့် အားနည်းချက်ဆိုင်ရာ မှတ်တမ်းများ (CWE) ပါဝင်အောင် လုပ်ထားသင့်ပါသည်။ CVE မှတ်တမ်းတိုင်း မှန်ကန် ပည့်စုံမှုရှိမရှိ သချော ဆောင်ရွက်ရာတွင် အချိန်ကဩမြင့်နိုင်သော်လည်း ထိုလုပ်ရပ်သည် မတူညီသည့် လုပ်ငန်းများမှ ခတော်ရစီးကဩောင်းကို ခန့်မှန်းသိစနိုင်ပီး ကုန်ထုတ်လုပ်သူများနှင့် ဝယ်ယူသုံးစွဲသူအတွက်ပါ အကျိုးရှိစမည်ဖစ်ပါသည်။ အာနည်းချက်ကို စီမံခဲ့ခြင်းဆိုင်ရာနှင့် ပတ်သက်၍ ပိုမိုသိလိုပါက CISA ၏ Stakeholder– specific SVCC guidance တွင် လေ့လာနိုင်ပါသည်။
- အလွှာအဆင့်ဆင့်ဖင့် နက်ရှိုင်းစွာ ကာကွယ်ထားခဲ့ပီး (Defence–in–Depth) – လုံခုံရေး ထိန်းချုပ်မှုတစ်ခု တိုက်ခိုက်ခံရမှုမှအစ စနစ်တစ်ခုလုံး တိုက်ခိုက်ခံရမှု မဖစ်စရေန်အတွက် အလွှာအဆင့်ဆင့်ဖင့် နက်ရှိုင်းစွာ ကာကွယ်ထားသည့် ဒီဇိုင်းဖင့် တည်ဆောက်ထားပါ။ ဥပမာ အသုံးပုခြင့် ကန့်သတ်ခဲ့ပီးနှင့် အချက်အလက်ရယူနိုင်မည့်သူများကို ကန့်သတ်ခဲ့ပီးသည်

[3] အချို့သော အာဏာပိုင် အဖွဲ့ဝင်စီများသည် ဆော့ဖ်ဝဲ ထုတ်လုပ်ရောင်းချရေးတွင် လုံခုံရေးဆိုင်ရာ အာမခံချက် ရရှိရန်အတွက် အခြားနည်းလမ်းများကို ရှာဖွေလျော် ရှိပါသည်။

အကာင့်တိုက်ခိုက်ခံရမှုများကို လျှော့ကျစေနိုင်ပါသည်။ ထို့အပြင် ဆော့ဖ်ဝဲများအားတစ်ခုချင်းစီခွဲခြားရယူမှုလုပ်ထားခြင်းအားဖြင့် စနစ်တစ်ခုလုံး တိုက်ခိုက်မှုမဖစ်စေရန် ကာကွယ်ပေးရာ ရောက်ပါသည်။

- စိတ်ကျနေပ်ဖွယ်ရာကောင်းသော ဆိုက်ဘာစွမ်းဆောင်မှုဆိုင်ရာ ရည်မှန်းချက်များ (Satisfy Cyber Performance Goals (CPGs))– အခြေခံ လုံခုံရြေးဆိုင်ရာ လုပ်ထုံးလုပ်နည်းနှင့် ကိုက်ညီသည့် ဆော့ဖ်ဝဲကို တီထွင်ပါ။ CISA ၏ ဆိုက်ဘာလုံခုံရြေးဆိုင်ရာ စွမ်းဆောင်မှ ရည်မှန်းချက်များ သည် အဖွဲ့အစည်းများမှ ထည့်သွင်းလုပ်ဆောင်သင့်သည့် အခြေခံ ဆိုက်ဘာကာကွယ်ရေး လုပ်ထုံးလုပ်နည်းများကို ဖော်ပြထားပါသည်။

ထို့အပြင် သင့်အဖွဲ့အစည်း၏ အနအေထားအား ပိုမိုခိုင်မာစရေန်အတွက် CSIA ၏ CPG နှင့် ဆင်တူသော UK ၏ ဆိုက်ဘာ ဆန်းစစ်အကဲဖြတ်မှုဆိုင်ရာ မူဘောင် (Cyber Assessment Framework) ကိုလည်း လေ့လာနိုင်ပါသည်။ အကယ်၍ ကုန်ထုတ်လုပ်သူများမှ ဆိုက်ဘာလုံခုံရြေးဆိုင်ရာ စွမ်းဆောင်မှ ရည်မှန်းချက်များ CPG နှင့်အညီ ဆောင်ရွက်မှမရှိလျင် – ဥပမာ အမူထမ်းအားလုံးအတွက် လှည့်စားဖြားယောင်းမှုကို ကာကွယ်ရန် တဆင့်ခံ စိစစ်မှုမျိုး မရှိခြင်းသည် – ထိုကုန်ပစ္စည်းများကို လုံခုံခြောင် ပုံပြင်စီမံထားသည့် ပစ္စည်းဟု မဆိုနိုင်ပါ။

အာဏာပိုင် အဂျင်စီများအနဖြင့် ထိုအပြောင်းအလဲများသည် အဖွဲ့အစည်းများ၏ အနအေထားကို သိသာစွာ ပြောင်းလဲမှုဖစ်စသေည်ကို သဘောပေါက်ပါသည်။ အရေးကြီးမှု၊ ခက်ခဲရှုတ်ထွေးမှုနှင့် စီးပွားရေးအပေါ် သက်ရောက်မှုကို အခြေခံပီးြ ဦးတို့၏ လုံခုံရြေး အစီအစဉ်ကို အစပေပိုင်းကတည်းက ဦးစားပေး လုပ်ရမည်ဖစ်ပါသည်။ ထိုလုပ်ထုံးလုပ်နည်းများကို ဆော့ဖ်ဝဲအသစ်အတွက် အသုံးပုနှိုင်သည့်အပြင် သမားရိုးကျဆော့ဖ်ဝဲနှင့် ကုန်ပစ္စည်းအတွက်ပါ တိုးချဲ့အသုံးပုမြှလည်း လုပ်နိုင်ပါသည်။ တချို့ ကိစ္စရပ်များတွင် ကုန်ပစ္စည်းတစ်ခု၏ အရေးကြီးမှုနှင့် ကုံရြှိနိုင်သည့် အခက်အခဲအနအေထားကခြောင့် ထိုလုပ်ထုံးလုပ်နည်းများကို အလျင်အမန်ြ အသုံးပုမြှ ဖစ်စနေိုင်ပါသည်။ တချိုအတွက် ထိုလုပ်ထုံးလုပ်နည်းများသည် တဆင့်ချင်း လုပ်ဆောင်ရမည် ဖစ်ပါသည်။

အလိုအလျောက် လုံခုံစြာ ရှိနခေြင်း၏ ဗျူဟာများ

ဆော့ဖ်ဝဲများ ထုတ်လုပ်ရာတွင် ကုန်ထုတ်လုပ်သူများအနဖြင့် လုံခုံခြောင် ပငြ်ဆင်စီမံထားသည့် လုပ်ထုံးလုပ်နည်းများ (Secure-by-Design) ကို အသုံးပုသြည့်အပြင် အလိုအလျောက် လုံခုံစြာ ရှိနခေြင်း (Secure-by-Default) နည်းကိုပါ ဦးစားပေးရန် အာဏာပိုင် အဂျင်စီများ အကံပြုပြုပါသည်။ ၎င်းသည် ဆော့ဖ်ဝဲများကို ခတော်နှင့်အညီ ပြောင်းသည့်အခါတွင်လည်း ထိုလုပ်ထုံးလုပ်နည်းများနှင့် လိုက်လျောညီထွမေှု ဖစ်စနေိုင်ပါသည်။ ဥပမာ –

- Eliminate default passwords (အလိုအလျောက် password ထားရှိပေးခြင်းကို မလုပ်ရန်) – လူတိုင်းမျှဝေသုံးစွဲနိုင်သည့် password လျှိုဝှက်နံပတ်များကို ကုန်ပစ္စည်းတွင် အလိုအလျောက် ထားရှိပေးခြင်းမျိုး မလုပ်သင့်ပါ။ အလိုအလျောက် password ထားရှိပေးခြင် မလုပ်ရန်အတွက် အာဏာပိုင် အဂျင်စီအနဖြင့်

အကဲဖြတ်သည်မှာ ဆင့်ဖဲ့ထဲ ထည့်သွင်းချိန်နှင့် ပုံဖော်ချိန်တွင် ဆင့်ဖဲ့ထဲအသုံးပြုမည့်သူများအား ခိုင်မာသည့် password များ ထားရှိပြီးမှ အသုံးပုံန်ိုင်အောင် ပုဂ္ဂိုလ်သင့်ကြောင်း အကဲဖြတ်ပါသည်။

- အထူးအသုံးပြုသူများအတွက် အချက်အလက်အမျိုးမျိုး မှန်ကန်ကြောင်း အထောက်အထား (Multifactor Authentication (MFA)) ကို ပဋိဉာန်းရမည်ဖြစ်သည်။ လုပ်ငန်းအများအပြားမှ တာဝန်ရှိသူများသည် ၎င်းတို့၏ အကောင့်များကို MFA နည်းဖဲ့ခြင်း ကာကွယ်မှု မလုပ်ထားကြောင်း ကျွန်ုပ်တို့အနေဖဲ့ခြင်း လေ့လာသိရှိရပါသည်။ တာဝန်ရှိသူများသည် ပစ်မှတ်ထားခံရနိုင်ခဲ့မြားသည့်အတွက် MFA တွင် ပါဝင်မည့်အစား ဖယ်ထားသင့်ပါသည်။ ထို့အပြင် တာဝန်ရှိသူအား MFA လုပ်ဆောင်ရန် ပုံမှန်စခိုင်းသင့်ပြီးငြင်းတို့၏ အကောင့်တွင် အောင်မငြိစွာ လုပ်ဆောင်နိုင်သည်အထိ လုပ်ခိုင်းသင့်ပါသည်။ နယ်သာလန်၏ NCSC လမ်းညွှန်မှုသည် CISA ၏ လမ်းညွှန်မှုနှင့် တူညီနပေါ်ြငင်းတို့၏ အချက်အလက်များပိုမိုသိလိုလျင် Mature Authentication Factsheet တွင် ကည့်ရှုနိုင်ပါသည်။

- တစ်ကိမြိလဲ့အင်ဝင်ခငြိး (Single sign-on (SSO)) – အိုင်တီများအနဖေဖဲ့ ခတော်မှီသဲ့ စံချိန်စံညွှန်းမှတဆင့် တစ်ကိမြိလဲ့အင်ဝင်နိုင်သည့် နည်းပညာကို အသုံးပြုင့်ပါသည်။ ဥပမာ Security Assertion Markup Language (SAML) နှင့် OpenID Connect (OIDC) တို့ ဖစ်ပါသည်။ ထိုအရာကို ထပ်မံကုန်ကျခံစရာမလိုအောင် အလိုအလျောက် လုပ်ဆောင်ပးသင့်ပါသည်။

- လုံခံ့ဖြာလဲ့အင်ဝင်ထားခငြိး (Secure Logging) – သုံးစွဲသူများထံမှ အဖိုးအခ ထပ်တောင်းခံမှုမလုပ်ပဲ အရည်အသွေးမဖဲ့သဲ့ ဝဘ်ဆိုက်လုပ်ရှားမှုမှတ်တမ်းကို လုပ်ဆောင်နိုင်ပါသည်။ ဝဘ်ဆိုက်လုပ်ရှားမှ မှတ်တမ်းသည် လုံခံ့ခြေးချိုးဖောက်မှု ခံရနိုင်သည့်အရာကို သိရှိအောင် လုပ်ဆောင်ရာတွင် အင်မတန် အရေးပါသည်။ လုံခံ့ခြေး ချိုးဖောက်မှု ဖစ်မဖစ် သံသယဖစ်နသေည့်အချိန် သို့မဟုတ် အတည်ပုဖြို့ စုံစမ်းနချိန်အတွက်လည်း အရေးပါပါသည်။ လုံခံ့ခြေးအချက်အလက်များနှင့် ဖစ်ရပ်စီမံခန့်ခဲ့မှု (SIEM) စနစ်များကို ကမ္ဘာတလွှား၏ ကိုဩဒိနိတ်အချိန် (UTC)။ စံသတ်မှတ်ထားသဲ့ နယ်မခြေအချိန်ပုံစံနှင့် ခိုင်မာသဲ့မှတ်တမ်းတင်ခငြိးနည်းလမ်းများကို အသုံးပုဩည့် application programming interface (API) နှင့် အလွယ်တကူပဝင်ိုးစည်းအသုံးပုခြငြိးကဲ့သို့ အကောင်းဆုံး လုပ်ထုံးလုပ်နည်းများကို ထည့်သွင်းစဉ်းစားပါ။

- ဆင့်ဖဲ့ဝဲ ခွင့်ပုခြွင်းမှု (Software Authorization Profile) – ဆင့်ဖဲ့ဝဲထုတ်လုပ်သူများအနဖေဖဲ့ ခွင့်ပုခြွင်းရရှိသည့်ပုဂ္ဂိုလ်များနှင့် ၎င်းအလုပ်အတွက် လိုအပ်သည့်အချက်များကိုသာ ယူခွင့်ရရန် လုပ်သင့်ပါသည်။ သတ်မှတ်ထားသည့် ခွင့်ပုခြွင်းမရှိပဲ ဝင်ရောက်ပါက အန္တရာယ်ရှိကြောင်း သိသာသည့် သတိပဲးမှုများ လုပ်ဆောင်ပးသင့်ပါသည်။ ဥပမာ – ဆရာဝန်သည် လူနာ၏ ကျန်းမာရေးဆိုင်ရာ မှတ်တမ်းများအားလုံးကို ကည့်ရှုခွင့်ရှိသဲ့လည်း ကျန်းမာရေး အချိန်ဇယား ရေးဆွဲသူသည် ရက်ချိန်းအချိန်ဇယားရေးဆွဲရန်အတွက် အချက်အလက်မှ လွဲ၍ ကျန်အချက်များ ဝင်မကည့်နိုင်ရင် လုပ်ဆောင်ခငြိးမျိုး ဖစ်ပါသည်။

- Forward-looking security over backwards compatibility – ခတော်ဟောင်း ဆင့်ဖဲ့ဝဲများသည် လုံခုံရြေးဆိုင်ရာအတွက် အန္တရာယ်ရှိစနိုင်သော်လည်း ၎င်းတို့ကို ဆက်လက်ထည့်သွင်း အသုံးပုနြိုင်ရန် လုပ်ဆောင်ထားလျက် ရှိပါသည်။ ဆင့်ဖဲ့ဝဲဟောင်းများကို ခတော်နှင့်အညီ ပန်ြိလည်သုံးစွဲနိုင်ရန် လုပ်ဆောင်ခငြိုးထက် လုံခုံရြေးကို ဦးစားပေးရမည် ဖစြိသကဲ့သို လုံခုံရြေးအသင်းသားများကိုလည်း လုံခုံမြှမရှိသည့် အရာများကို ဖယ်ရှားခွင့်ပေးရမည်ဖစြိပီးြထိုကဲ့သို့ ဖယ်ရှားမှုသည် လုပ်ငန်းအပြောင်းအလဲများ ဖစြိစသေည့်တိုင်အောင် ဖယ်ရှားခွင့် ပေးသင့်ပါသည်။
- တင်းကပြိမှုအရွယ်အစားကို ခြရောခံပီးြလျှော့ချခငြိုး (Track and reduce “hardening guide” size) – တင်းကပြိမှု အရွယ်အစားအား လျှော့ချပီးြပုံစံသစ် ဆင့်ဖဲ့ဝဲများ ထုတ်လုပ်သည့်အခါတွင် တင်းကပြိမှုအရွယ်အစားကို တဖြေးဖြေးချည်းစီ လျှော့ချနိုင်ရန် လုပ်ဆောင်သင့်ပါသည်။ တင်းကပြိခငြိုးကို ကုန်ပစ္စည်းထုတ်လုပ်ရေးအတွက် ပူးတွဲထည့်တွင်းရမည့်အရာအဖစြိ အသုံးပုြင့်ပါသည်။ အာဏာပိုင် အဂြေင်စီများအနဖေြ့ ဝယ်ယူသုံးစွဲသူများနှင့် ထားရှိသည့် မိတ်ဆက်ဆက်ဆံရေး၊ ကုန်ထုတ်လုပ်သူအသင်းများ၏ ကိုုိယ်စားဆောင်ရွက်မှုနှင့် ဝယ်ယူသုံးစွဲသူများ၏ အတွ့အကုံမြှတ်ချက်များသည် တင်းကပြိမှုကို အချိန်တိုအတွင်း လျှော့ချမှုဖစြိစနိုင်သည်ကို သဘာဝပေါက်နားလည်ပါသည်။
- သုံးစွဲသူအတွ့အကုံြအကျိုးသက်ရောက်မှုဆိုင်ရာ လုံခုံရြေးအနအေထားကိုလည်း ထည့်သွင်းစဉ်းစားရန် လိုအပ်ပါသည်။ လုံခုံရြေး setting တိုင်းသည် အသုံးပုသြူများအတွက် အပိုဝန်ထုတ်ဖစြိစနိုင်သည့်အတွက် ထိုအချက်ကို
- စီးပွားရေးအကျိုးအမြတ်နည်းစနိုင်ခငြိုးနှင့် တိုက်ဆိုင်၍ အကဲဖတ်သင့်ပါသည်။ အကောင်းဆုံးအနအေထားအတွက် setting ရှိမနသေင့်ဘဲ ၎င်းအစား အကောင်းဆုံးလုံခုံမြှ setting ကိုသာလျင် နဂိုကတည်းက အလိုအလျောက် ထည့်သွင်းထားတာမျိုး ဖစြိသင့်ပါသည်။ ဖွံ့စည်းပုံစနစ် မဖစြိမနလေိုအပ်လာလျင် ဖစြိပ၏လာနိုင်သည့် ခိမြိုးခြောက်မှုအန္တရာယ်ကို အလိုအလျောက် ကာကွယ်ပီးြသနေည်းကို အသုံးပုြင့်ပါသည်။

အာဏာပိုင် အဂြေင်စီများအနဖေြ့ ထိုအပြောင်းအလဲများသည် ဆင့်ဖဲ့ဝဲအသုံးပုခြငြိုးဆိုင်ရာ လုပ်ငန်းလည်ပတ်ရေးအပ၏ သက်ရောက်မှုဖစြိနိုင်သည်ကို နားလည်ပါသည်။ ထို့ကြောင့် သုံးစွဲသူ၏ အသုံးပုမြှ အတွ့အကုံြသည် လုပ်ငန်းလည်ပတ်ရေးနှင့် လုံခုံရြေး ထိန်းညိမှုအတွက် အလွန်အရေးကီးြပါသည်။ အာဏာပိုင် အဂြေင်စီများ၏ အမငြိအရ ဆင့်ဖဲ့ဝဲလုံခုံရြေးရှိအောင် ဦးစားပေးလုပ်ကိုင်သည့် လုပ်ထုံးလုပ်နည်းသည် အဖွဲ့အစည်းအတွက် အရေးကီးြဆုံး လုပ်ဆောင်ရမည့် ပထမခငြေလှမ်းဖစြိပီးြထိုအိုင်ဒီယာများကို ဦးစားပေးသည့်အနဖေြ့ ထိပ်သီးခဝေါင်းဆောင်များသည် လမ်းပမြေငြပုံ ရေးဆွဲပီးြလုပ်ဆောင်သင့်ပါသည်။ ဝယ်ယူသုံးစွဲသူများ၏ သုံးစွဲမှုအတွ့အကုံြသည် အရေးကီးြသော်လည်း တခါတရံ အရည်အသွေးမငြိတင်ရန်အတွက် လုပ်ဆောင်ရာတွင် ဝယ်ယူသုံးစွဲသူများမှ ဝင်ရောက်ပါဝင်ခငြိုး မလုပ်လိုသည့် အနအေထားများ ရှိတတ်သည်ကိုလည်း အာဏာပိုင် အဂြေင်စီများအနဖေြ့ သတိပုမြိုပါသည်။ ထို့ကြောင့် ဝယ်ယူသုံးစွဲသူများသည် အားနည်းချက်ရှိသူအဖစြိ တသက်လုံး မဖစြိရလအောင် ခတော်ရစီးကြောင်းတွင် ပါဝင်လာစရေန်အတွက်

ကုန်ထုတ်လုပ်သူများအနေဖြင့် အဓိပ္ပာယ်ရှိသည့် မက်လုံးများဖြင့် ဝယ်ယူသုံးစွဲသူများအား ဆွဲဆောင်နိုင်ရန် ပူဖြုပ်သင့်ပါသည်။

တင်းကပ်မှု နှင့် ဖြေလျှော့မှု လမ်းညွှန်ချက်များ (HARDENING VS LOOSENING GUIDES)

ဆော့ဖ်ဝဲထုတ်လုပ်ရန် စီစဉ်ရေးဆွဲချိန်မှစ၍ လုံခုံခြောကင်းသော ထိန်းချုပ်မှုကို ခိုင်ခံ့စွာ မလုပ်ဆောင်သည့်အတွက် တင်းကပ်မှုလမ်းညွှန်ချက်များ (hardening guides) ကို လိုအပ်ခြင်း ဖစ်စေနိုင်သည်။ တဖက်တွင်လည်း ထိုတင်းကပ်မှုလမ်းညွှန်ချက်များသည် လုံခုံမြဲမရှိသောအရာများ၏ တိုက်ခိုက်ခံရနိုင်ခြေရှိမှုကို သိသာစေသည့် လမ်းပမြေပုံလည်း ဖစ်စေနိုင်ပါသည်။ အဖွဲ့အစည်းအများအပြားအနေဖြင့် တင်းကပ်ရေးလမ်းညွှန်ချက်များကို နားမလည်သည့်အတွက် ၎င်းတို့၏ ကုန်ပစ္စည်းများကို မလုံခုံဖြည့်အနအေထား ဖစ်စေနိုင်ပါသည်။ တဖက်တွင် ထိုတင်းကပ်မှုလမ်းညွှန်ချက်များအစား ဖြေလျှော့မှုလမ်းညွှန်ချက်ကို အသုံးပုဖြင့်ပါသည်၊ မည်သည့်အရာကို ပြောင်းလဲသင့်ကြောင်း ရှင်းပဖြေက်သာမက ဖစ်နိုင်ခြေရှိသည့် လုံခုံရေးခိမြိုးခြောက်မှုကိုလည်း မှတ်တမ်းတင်ထားသင့်ပါသည်။

ကုန်ပစ္စည်းလုံခုံရေးအတွက် တင်းကပ်မှုလမ်းညွှန်ချက်များကို ဖန်တီးမည့်အစား အလိုအလျောက် လုံခုံမြဲရှိနခေြင်း နည်းလမ်းကို အသုံးပုရန် အာဏာပိုင်အဖျော်စီများအနေဖြင့် ကုန်ထုတ်လုပ်သူများအား အကံပြုလိုပါသည်။ ထိုလမ်းညွှန်ချက်များသည် ဆိုက်ဘာတိုက်ခိုက်မှု၏ အနှတရာယ်အကြောင်းကို လုပ်ငန်းရှင်များ နားလည်သဘောပေါက်ရန် ရိုးရှင်းပီြနားလည်လွယ်သော ဘာသာစကားများဖြင့် ရှင်းပြောပါသည်။ လုံခုံရေးဆိုင်ရာအချက်များကို အလျှော့အတင်း လုပ်မည်ဆိုပါက ဝယ်ယူသုံးစွဲသူများဆိုင်ရာ အကြီြအကဲများ၏ ဆုံးဖြတ်ချက်ရယူသင့်ပီြအခြေးသော စီးပွားလုံးငန်း၏ လုံခုံရေးနှင့် ထိန်းညိလုပ်ဆောင်ရမည် ဖစ်ပါသည်။

ဝယ်ယူသုံးစွဲသူများအတွက် အကံပြုချက်များ

အာဏာပိုင်အဖျော်စီများအနေဖြင့် စက်မှုကုန်ထုတ်လုပ်သူများအား အကံပြုလိုသည်မှာ ၎င်းတို့ ထုတ်လုပ်သည့် စက်မှုပစ္စည်းများ၏ လုံခုံရေးနှင့် ပတ်သက်၍ တာဝန်ယူမှု တာဝန်ခံမှ ရှိသင့်ပါသည်။ ထိုသို့လုပ်ဆောင်ရန်အတွက် လုံခုံခြောင် ပငြိဆင်စီမံထားသည့် ကုန်ပစ္စည်းနှင့် အလိုအလျောက် လုံခုံမြဲရှိနသေည့် ကုန်ပစ္စည်းများကို ဝယ်ယူအသုံးပုရန် အရေးကီြးသည့်အကြောင်းကို အဖွဲ့အစည်း၏ ထိပ်သီးပုဂ္ဂိုလ်များမှ ဦးစားပေးလုပ်ဆောင်ရန် လိုအပ်ကြောင်း အကံပြုလိုပါသည်။ လိုအပ်လျှင် ဝယ်ယူမှု မလုပ်မီအချိန်မှစ၍ အိုင်တီဌာနများအနေဖြင့် ဆော့ဖ်ဝဲကုန်ထုတ်လုပ်သူများ၏ ကုန်ပစ္စည်းလုံခုံမြဲကို ဆန်းစစ်မှုပူဖြုပ်ခွင့်ပေးမည့် မူဝါဒများချမှတ်ပီြးလုပ်ဆောင်သင့်ပါသည်။ လုံခုံခြောင် ပငြိဆင်စီမံထားသည့်ကုန်နှင့် အလိုအလျောက် လုံခုံမြဲရှိနသော ကုန်များတွင် (ဤစာစောင်တွင် ဖော်ပြထားသည့်အရာများအပငြိ အခြေးအဖွဲ့အစည်းများ၏ ဖော်ပခြက်များအပါအဝင် ဖစ်ပါသည်) ရှိသင့်သည့် စံချိန်စံနှုန်းများကို သတ်မှတ်ဆုံးဖြတ်ရာတွင် အိုင်တီ ဌာနကို ဆုံးဖြတ်ခွင့်ပေးသင့်ပါသည်။ ထိုကဲ့သို့ ဝယ်ယူမှု ဆုံးဖြတ်ချက်များကို အိုင်တီဌာနမှ ချမှတ်အကံပြုခြည့်အခါတွင်လည်း

ထိပ်သီးစီမံအုပ်ချုပ်သူ အရာရှိများ၏ ထောက်ခံအားပေးမှု လိုအပ်ပါသည်။ စက်မှုကုန်ပစ္စည်းများအတွက် လုံခြုံရေးဆိုင်ရာနှင့် ပတ်သက်၍ ကုံရှုနိုင်သည့် အခက်အခဲများကိုလည်း မှတ်တမ်းတင်ထားတင်သကဲ့သို့ အဖွဲ့အစည်း၏ ဆုံးဖြတ်ချက်အားလည်း မှတ်တမ်းတင်ထားသင့်ပါသည်၊ ထိုမှတ်တမ်းတင်မှုကိုလည်း အကြီးတန်းစီးပွားရေး အမှုဆောင်အရာရှိများ၏ သဘောတူညီချက်ရရှိမှုလိုအပ်ပြီး၊ ထိုအရာများကိုလည်း ဒါရိုက်တာ ဘုတ်အဖွဲ့ကို ပုံမှန်တင်ပြမှု လုပ်သင့်ပါသည်။

ကုမ္ပဏီ၏ ဒေတာကွန်ရက်၊ အိုင်ဒီနှင့် အချက်အလက်ရယူခွင့်ဆိုင်ရာ စီမံမှု၊ လုံခြုံရေးဆိုင်ရာ၊ လုပ်ကိုင်နိုင်စွမ်းအပေါ် တုန့်ပြန်မှု စသည့် လုပ်ငန်း၏ လုံခြုံရေးဆိုင်ရာ အနေအထားကို ပံ့ပိုးပေးသည့် ကုမ္ပဏီ၏ အိုင်တီ ဝန်ဆောင်မှုကို အရေးကြီးသည့် လုပ်ငန်း၏ အစိတ်အပိုင်းအဖြစ် သတ်မှတ်ပြီး၊ လုပ်ငန်း၏ ရည်မှန်းချက် အောင်မြင်မှုနဲ့ ကိုက်ညီစေမည့် ငွေကြေးများ ထားရှိသုံးစွဲမှု လုပ်နိုင်ရမည် ဖြစ်သည်။ လုံခြုံအောင် ပြင်ဆင်စီမံခြင်းနှင့် အလိုအလျောက် လုံခြုံမှုရှိနေသော ကုန်ပစ္စည်းများကို ကုန်ထုတ်လုပ်သူများ ထုတ်လုပ်နိုင်စွမ်းရှိရန်အတွက်လည်း အဖွဲ့အစည်းများမှ အစီအစဥ်များ ရေးဆွဲပြီး၊ တိုးတက်မှုရှိအောင် ပံ့ပိုးပေးရမည် ဖြစ်သည်။

ဖြစ်နိုင်ပါက ကုမ္ပဏီများအနေဖြင့် ၎င်းတို့၏ အဓိက အိုင်တီပစ္စည်း ရောင်းချသူအဖွဲ့နှင့် ဗျူဟာကျကျ မိတ်ဖက်မှုရှိအောင် ကြိုးစားလုပ်ဆောင်သင့်ပါသည်။ ထိုမိတ်ဖက်ချိတ်ဆက်မှုများသည် အလွှာအသီးသီးရှိသည့် အဖွဲ့အစည်းများနှင့် ယုံကြည်မှုရယူခြင်းများပါဝင်ပြီး၊ ပြဿနာ ကုံရှုသည့်အချိန် သို့မဟုတ် ဘုံဦးစားပေးစရာများရှိသည့်အခါတွင် အပြန်အလှန်ဖေးဖေးမမ လုပ်ဆောင်နိုင်ကမြည် ဖြစ်ပါသည်။ ထိုကဲ့သို့ မိတ်ဖက်ဆက်ဆံမှုများတွင် လုံခြုံရေးကို အဓိကထားရမည်ဖြစ်ပြီး၊ လုံခြုံအောင် ပြင်ဆင်စီမံခြင်းနှင့် အလိုအလျောက် လုံခြုံခြေင်း၏ လုပ်ထုံးလုပ်နည်းများကို အလေးထားကျင့်သုံးနိုင်ရန်အတွက် ချိတ်ဆက်ထားရန်ဖြစ်ပြီး၊ အတည်တကျ တရားဝင်နည်း (ဥပမာ စာချုပ်နှင့်တကွ သို့မဟုတ် ရောင်းဝယ်ရေးသဘောတူစာချုပ်) ဖြစ်စေ ရိုးရိုးနှုတ်အရ သဘောတူညီမှုဖြစ်စေ လုပ်ဆောင်ထားသင့်ပါသည်။ စက်မှုပစ္စည်းထုတ်လုပ်ရောင်းချသူများသည်လည်း ၎င်းတို့၏ လုံခြုံမှုထိန်းချုပ်ရေး အနေအထားနှင့် လုံခြုံအောင် ပြင်ဆင်စီမံထားခြင်းနှင့် အလိုအလျောက် လုံခြုံမှုရှိနေခြေင်း လုပ်ထုံးလုပ်နည်းဆိုင်ရာ လမ်းပြမြေပုံနှင့် ဆက်စပ်ပြီး ကုမ္ပဏီများကို ပွင့်လင်းမြင်သာမှုရှိအောင် ချပြသင့်ပါသည်။

အဖွဲ့အစည်းအတွင်း လုံခြုံအောင် ပြင်ဆင်စီမံခြင်းကို ဦးစားပေးအရာအဖြစ် လုပ်ဆောင်သည့်အပြင် အိုင်တီ အကြီးအကဲများအနေဖြင့် ၎င်းတို့နှင့် လုပ်ငန်းတူ လုပ်ကိုင်သူများနှင့် ပူးပေါင်းမှု ရယူ၍ ထိုလုံခြုံရေးအခြခံမှုများ အကောင်အထည်ဖော် လုပ်ဆောင်ရန်အတွက် မည့်သည့်ကုန်ပစ္စည်းနှင့် ဝန်ဆောင်မှုက အကောင်းဆုံးဖြစ်သည့်အကြောင်း နားလည်သဘောပေါက်ရန် ပူးပေါင်းမှုရယူသင့်ပါသည်။ ဆော့ဖ်ဝဲကုန်ထုတ်လုပ်သူများအနေဖြင့် နောက်နောင်ထုတ်လုပ်မည့်ကုန်များတွင် လုံခြုံရေးကို ဦးစားပေးနိုင်ရန်အတွက် ခေါင်းဆောင်များမှ ပူးပေါင်း၍ တင်ပြတောင်းဆိုမှုများ ပြုလုပ်သင့်ပါသည်။ အတူတူ ပူးပေါင်းလုပ်ကိုင် ဆောင်ရွက်ခြင်းအားဖြင့် သုံးစွဲသူများသည် ကုန်ထုတ်လုပ်သူများအတွက် အသုံးဝင်သည့် အကြံဉာဏ်များ ပေးနိုင်သည့်အပြင် ကုန်ထုတ်လုပ်သူများအား လုံခြုံရေးကို ဦးစားပေးအောင် လှုံ့ဆော်မှုများလည်း ဖြစ်စေနိုင်ပါသည်။
Cloud system ကို အသုံးပြုသည့်အချိန်တွင် အဖွဲ့အစည်းများသည် စက်မှုပစ္စည်းရောင်းချပံ့ပိုးသူများနှင့် တာဝန်ခွဲယူမှုရှိသင့်ကြောင်းကို နားလည်ရန် အရေးကြီးပါသည်။ လုံခြုံရေးဆိုင်ရာ တာဝန်ကို

စက်မှုထုတ်လုပ်သူများမှ တာဝန်ယူရမည်ဖစ်ပြီး၊သုံးစွဲသူ၏ တာဝန်သက်သက်မဟုတ်ကြောင်းကို အဖွဲ့အစည်းများမှ ရှင်းလင်းအောင် လုပ်ဆောင်ထားရမည်ဖစ်သည်။ ထို့ကြောင့် ၎င်းတို့၏ လုံခုံရြေးအနအေထားကို ပွင့်လင်းမငြ်သာမှုရှိအောင်လုပ်ဆောင်ထားသည့် ဆဇ့ေဖ်ဝဲဝန်ဆောင်မှုပးေသူများ၊ ဌာနတွင်း လုံခုံရြေးထိန်းချုပ်မှု၊ ၎င်းတို့၏ ပူးတွဲတာဝန်ဝတ္တရားကို ထမ်းဆောင်မှုပးေနိုင်သည့် အဖွဲ့နှင့် ဦးစားပး ေပူးပါင်းလုပ်ဆောင်ရန် အဖွဲ့အစည်းများကို အကံပြုတြိုပါသည်။

မသက်ဆိုင်ကြောင်း ရှင်းလင်းချက်

ဤအစီရင်ခံစာပါ အချက်အလက်များသည် “ဤကဲ့သို့" အချက်အလက်အသိပးေခြင်းရည်ရွယ်ချက်အနဖေြင့်သာ ဖော်ပြထားခြင်း ဖစ်ပါသည်။ CISA နှင့် အာဏာပိုင် အဂျင်စီများသည် မည်သည့် ထုတ်ကုန်၊ မည်သည့်ဝန်ဆောင်မှု၊ မည်သည့် လင့်လာဆန်းစစ်စိတ်ဖြာမှုကိုမှ ထောက်ခံမှု မလုပ်ထားပါ။ ကုမ္ပဏီ၏ နာမည် သို့မဟုတ် ပစ္စည်းတစ်ခု၏ နာမည်၊ သို့မဟုတ် လုပ်ငန်းစဉ် သို့မဟုတ် ဝန်ဆောင်မှု၊ ကုန်အမှတ်တံဆိပ်၏ နာမည်၊ ကုန်ထုတ်လုပ်သူ၏ နာမည်နှင့် အခြားနာမည်များကို ဖော်ပြခြင်သည်ရှိသော် ၎င်းတို့ကို CISA နှင့် အာဏာပိုင်အဂျင်စီမှ ထောက်ခံချက်ပးေခြင်း၊ သုံးစွဲရန် အကံပြုခြင်း သို့မဟုတ် မျက်နှာသာပးေခြင်း မဟုတ်ကြောင်း အသိပးေလိုပါသည်။ ဤစာစောင်သည် CISA ၏ ဦးဆောင် ပူးပါင်းဆောင်ရွက်မှု စာစောင်ဖစ်ပြီးစည်းမျဉ်းစည်းကမ်းနှင့်တကွ လိုက်နာရမည့် စာစောင်မဟုတ်ကြောင်းကိုလည်း သတိပးေအပ်ပါသည်။

ကျမ်းကိုးစာများ

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
- လုံခုံမြဲမရှိတဲ့ စက်မှုပစ္စည်းအသုံးပုခြင်းအတွက် ကုန်ကျစရိတ်နဲ့ ဒါကို ဘယ်လိုဖခြေရှင်းရမလဲ – CISA
- ဆိုက်ဘာလုံခုံရြေးအတွက် ကုန်ကျစရိတ်ကို တဆင့်ကျခံစတောမျိုးကို ရပ်တန့်လိုက်ပါ – လုံခုံစြာ တီထွင်ခြင်းနည်းကို ဘာကြောင့် စက်မှုထုတ်ကုန် ကုမ္ပဏီတွေ ကျင့်သုံးသင့်သလဲ (foreignaffairs.com)
- CISA’s Stakeholder-Specific Vulnerability Categorization (SSVC) Guidance
- CISA’s Phishing Resistant MFA Fact Sheets
- အသးေစား စီးပွားရးေလုပ်ငန်းများအတွက် ဆိုက်ဘာလုံခုံရြေးဆိုင်ရာ လမ်းညွှန်ချက်များ Cyber | 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
- ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ တိုက်ခိုက်မှု – တုန့်ပြန်ခြင်းနှင့် တိုင်တန်းခြင်း
- FBI ၏ ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ ဗျူဟာ

သိုမဟုတ် စံနှုန်းများနှင့် နည်းပညာဆိုင်ရာ အမျိုးသားသိပ္ပံ (National Institute of Standards and Technology (NIST))

- NIST's Digital Identity Guidelines
- NIST ၏ ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ မူဘောင်
- NIST ၏ လုံခြုံမြဲရှိသော ဆော့ဖ်ဝဲထုတ်လုပ်ခြင်းဆိုင်ရာ မူဘောင် (SSDF)

ဩစတြေးလျ၏ ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ စင်တာ (ACSC)

- ACSC's IoT Code of Practice Guidance for Manufacturers

ယူကေ၏ တနိုင်လုံးဆိုင်ရာ ဆိုက်ဘာလုံခြုံရေးစင်တာ

- 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
- Cambridge တက္ကသိုလ်၏ CHERI
- So long and thanks for all the bits – NCSC.GOV.UK

ကနဒေါ၏ ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ စင်တာ (CCS)

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

ဂျာမနီနိုင်ငံ အချက်အလက် လုံခြုံရေးဆိုင်ရာဌာန (Germany's Federal Office for Information Security (BSI))

- The BSI Grundschutz compendium (module CON.8)
- The international standard IEC 62443, part 4–1
- ဂျာမနီ၏ အိုင်တီ လုံခြုံရေးအနအေထား အစီရင်ခံစာ –၂၀၂၂
- BSI practices of web application security

နယ်သာလန်၏ နိုင်ငံလုံးဆိုင်ရာ ဆိုက်ဘာ
လုံခြုံရေးစင်တာ

- NCSC–NL's Mature Authentication Factsheet

အခြား

- ရှုတ်ထွေတဲ့ စနစ်တွေ ဘယ်လို ကျဆုံးကြသလဲ
- The New Look in complex system failure