

နည်းပညာဗဟုသုတ စာတမ်း

Cybersecurity Supply Chain Risk Management Practices

မန်မာဘာသာ လေ့လာရေးလမ်းညွှန်

စနစ်များနှင့် အဖွဲ့အစည်းများအတွက်

NIST Special Publication 800-161 Rev. 1 Update 1 ကို အခြေခံ၍ အဓိကအယူအဆများ၊
စီမံခန့်ခွဲမှုအဆင့်များနှင့် လက်တွေ့လုပ်ဆောင်ရန် အချက်များကို မန်မာလို ပြန်လည်တင်ပြထားသည်။
မူရင်းထုတ်ဝေမှုမှာ ၂၀၂၂ ခုနှစ်ဖေဖော်ဝါရီလ ၂၄-၁၁-၀၁ အထိ ပြင်ဆင်ချက်များ ပါဝင်သည်။

ဤစာတမ်းသည် ဖတ်ရှုနားလည်လွယ်စေရန် ပြုပြင်ဆင်ခြင်မှုများ ပြုလုပ်ထားသော အကျဉ်းချုပ်နှင့် လက်တွေ့လမ်းညွှန်ဖြစ်သည်။ မူရင်း NIST စာတမ်း၏
စာမျက်နှာတိုင်းကို စာလုံးချင်းပြန်ဆိုထားသော အပြည့်အစုံဘာသာပြန်မဟုတ်ပါ။ အကောင်အထည်ဖော်ရာတွင် မူရင်း NIST
စာတမ်းနှင့် သက်ဆိုင်ရာ ဥပဒေ၊ စံနှုန်းများကိုပါ စစ်ဆေးပါ။

၁။ စာတမ်း၏ရည်ရွယ်ချက်

အဖွဲ့အစည်းတစ်ခုသည် ကွန်ပျူတာ၊ ဆော့ဖ်ဝဲ၊ network ပစ္စည်း၊ cloud ဝန်ဆောင်မှု၊ သို့မဟုတ် ပြင်ဆင်ထိန်းသိမ်းရေးဝန်ဆောင်မှုကို ဝယ်ယူသည့်အခါ ယုံကြည်ရသော ထုတ်လုပ်သူတစ်ဦးတည်းနှင့်သာ ဆက်ဆံနေရောင်း မဟုတ်တတ်ပါ။ ထုတ်လုပ်သူ၏ ပေးသွင်းသူ၊ အစိတ်အပိုင်းထုတ်လုပ်သူ၊ ဆော့ဖ်ဝဲစာကဏ္ဍတိုက်၊ ဖန်တိုက်သူ၊ cloud နှင့် ပြင်ပဝန်ဆောင်မှုပေးသူများ အဆင့်ဆင့် ပါဝင်နိုင်သည်။

ဒီကွင်းဆက်တွဲတွင် ထုတ်ကုန်အတု၊ မလိုလားအပ်သော လုပ်ဆောင်ချက်၊ အားနည်းချက်ပါသော code၊ လုံခြုံမှုမရှိသော ဖွဲ့စည်းလုပ်ငန်းစဉ်၊ တစ်ဖက်အဖွဲ့အစည်း၏ ထိန်းချုပ်မှု၊ သို့မဟုတ် အထောက်အထားမရှင်းလင်းသော မူလရင်းမြစ်တို့ကြောင့် အန္တရာယ်ဖြစ်နိုင်သည်။ ဝယ်ယူသူက ပစ္စည်းကို ဘယ်လိုတည်ဆောက်ထားသည်၊ ဘယ်သူက ဝင်ရောက်ပြင်ဆင်သည်ဆိုတာကို မမြင်နိုင်ခြင်းက အန္တရာယ်ကို ရှာဖွေဖို့ ပိုခက်စေသည်။

NIST 800-161 က cybersecurity supply chain risk management (C-SCRM) ကို တစ်ကိမ္မာတည်း စစ်ဆေးပေးသည့် လုပ်ငန်းအဖွဲ့မဟုတ်ဘဲ၊ အဖွဲ့အစည်း၏ အန္တရာယ်စီမံခန့်ခွဲမှုထဲ ထည့်သွင်းဆောင်ရွက်ရမည့် ဆက်တိုက်လုပ်ငန်းစဉ်အဖွဲ့ ရှင်းပြထားသည်။

၂။ အဓိကဝေါဟာရများ

- **Supply chain** — ထုတ်ကုန် သို့မဟုတ် ဝန်ဆောင်မှုကို ဒီဇိုင်းဆွဲခြင်း၊ ဖန်တီးခြင်း၊ ပေါင်းစည်းခြင်း၊ ပို့ဆောင်ခြင်း၊ တပ်ဆင်ခြင်း၊ လည်ပတ်ထိန်းသိမ်းခြင်းနှင့် ဖယ်ရှားခြင်းအထိ ပါဝင်သည့် လူ၊ အဖွဲ့အစည်းနှင့် လုပ်ငန်းစဉ်များ။
- **C-SCRM** — ကွင်းဆက်တစ်လျှောက်ရှိ cybersecurity အန္တရာယ်များကို ဖော်ထုတ်၊ အကဲဖြတ်၊ ဦးစားပေးပြီး လျော့ချသည့် စီမံခန့်ခွဲမှု။
- **Supplier** — ပစ္စည်း၊ ဆော့ဖ်ဝဲ၊ အစိတ်အပိုင်း သို့မဟုတ် ဝန်ဆောင်မှုကို ပေးသည့် ကုမ္ပဏီ၊ အဖွဲ့အစည်း သို့မဟုတ် ပုဂ္ဂိုလ်။ **Supplier** တိုက်ရိုက်တစ်ဆင့်တည်းကိုသာ မကည့်ဘဲ အောက်ဆင့်ပေးသွင်းသူများကိုပါ စဉ်းစားရသည်။
- **Supply chain assurance** — ပစ္စည်း၏ မူလရင်းမြစ် တည်ဆောက်ပုံ၊ စမ်းသပ်မှုနှင့် လုပ်ငန်းစဉ်များကို သက်သေပြနိုင်သည့် ယုံကြည်စိတ်ချရမှု။

၃။ စီမံခန့်ခွဲမှုကို အဆင့်သုံးဆင့်ဖြင့် ချိတ်ဆက်ခြင်း

C-SCRM ကို အဖွဲ့အစည်းတစ်ခုလုံး၏ လုပ်ငန်းရည်မှန်းချက်နှင့် ဆုံးဖြတ်ချက်များထဲ ပေါင်းစည်းရန် NIST က အဆင့်သုံးဆင့်ကို ဖော်ပြသည်။ အဆင့်များသည် သီးခြားမဟုတ်ဘဲ အထက်အောက် သတင်းအချက်အလက်နှင့် တာဝန်များ အပြန်အလှန်စီးဆင်းရသည်။

အဆင့် ၁ — အဖွဲ့အစည်းတစ်ခုလုံး

ခေါင်းဆောင်ပိုင်းက အန္တရာယ်လက်ခံနိုင်မှု၊ C-SCRM မူဝါဒ၊ ရင်းနှီးမြှုပ်နှံမှု၊ တာဝန်ခံသူများနှင့် အဖွဲ့အစည်းအဖွဲ့ လိုက်နာရမည့် အခြေခံစည်းမျဉ်းများကို သတ်မှတ်သည်။ လုပ်ငန်း၊ လုံခြုံရေး၊ ဝယ်ယူရေး၊ ဥပဒေရေးရာနှင့် နည်းပညာဌာနများ ပူးပေါင်းနိုင်ရန် စီမံခန့်ခွဲမှုအဖွဲ့တစ်ခု သတ်မှတ်နိုင်သည်။

အဆင့် ၂ — လုပ်ငန်းတာဝန်နှင့် လုပ်ငန်းစဉ်

လုပ်ငန်းတစ်ခုစီ၏ အရေးပါမှု၊ ဝန်ဆောင်မှုပတ်ဝန်းကျင် ထိခိုက်မည့်အရာ၊ သုံးစွဲမည့်အချက်အလက်နှင့် လိုအပ်သော **supplier** များကို ဆန်းစစ်သည်။ အရေးကြီးလုပ်ငန်းအတွက် လက်ခံနိုင်သော **supplier** နှင့် နည်းပညာအန္တရာယ်ကို သတ်မှတ်ပြီး ဝယ်ယူရေးစည်းမျဉ်းထဲ ပေါင်းထည့်သည်။

အဆင့် ၃ — စနစ်နှင့် လုပ်ငန်းဆောင်ရွက်မှု

စနစ်တစ်ခုချင်းစီအတွက် **supplier**၊ ပစ္စည်း၊ **software dependency**၊ **network** ဆက်သွယ်မှု၊ အသုံးပစ္စည်း၊ **update** လုပ်ပုံ၊ အားနည်းချက်နှင့် အရေးပေါ်တုံ့ပြန်မှုကို စီမံသည်။ စနစ်ပိုင်ရှင်၊ လုံခြုံရေးအဖွဲ့နှင့် ဝန်ဆောင်မှုပေးသူတို့၏ တာဝန်များကို သတ်မှတ်ထားရသည်။

၄။ အန္တရာယ်စီမံမှု စက်ဝန်း — Frame, Assess, Respond, Monitor

Frame — အခြေအနေနှင့် စည်းမျဉ်းဘောင် သတ်မှတ်ခြင်း

ဘယ်လုပ်ငန်း၊ စနစ်နှင့် ပေးသွင်းသူတွင် အရေးကြီးသလဲ၊ အဖွဲ့အစည်းက ဘယ်လောက်အန္တရာယ်ကို လက်ခံနိုင်သလဲ၊ ဥပဒေ၊ စာချုပ်နှင့် လုပ်ငန်းလိုအပ်ချက်တွင် ဘာတွင်သတ်မှတ်ထားသလဲဆိုတာ ရှင်းလင်းစေသည်။ ပိုင်ရှင်၊ ဆုံးဖြတ်ခွင့်နှင့် အန္တရာယ်တင်ပြမှုလမ်းကဏ္ဍကို သတ်မှတ်ပါ။

Assess — အန္တရာယ်အကဲဖြတ်ခြင်း

ပစ္စည်း/ဝန်ဆောင်မှု၏ အရေးပါမှု၊ **supplier** နှင့် အောက်ဆင့် **supplier** များ၊ မူလရင်းမစ်၊ ခြိမ်းခြောက်သူ၊ အားနည်းချက်၊ ဖြိုခွဲခြင်းနှင့် ဖြိုလာလျှင် ထိခိုက်မှုတို့ကို စုဆောင်းသုံးသပ်သည်။ သက်သေခံသည့်အချက်ကို အမှန်တရားအဖြစ် မယူဆဘဲ မသေချာမှုကို မှတ်တမ်းတင်ပါ။

Respond — တုံ့ပြန်မှုအန္တရာယ်လျှော့ချခြင်း

အန္တရာယ်ကို လက်ခံမည်၊ လျှော့ချမည်၊ အစိုးရနှင့် ခွဲဝေမည်၊ သိမ္မဟုတ် ဝယ်ယူမှု/အသုံးပြုမှုကို

ရှောင်ရှားမည်ကို သက်ဆိုင်ရာအာဏာပိုင်က ဆုံးဖြတ်သည်။ ထိန်းချုပ်မှုများ၊ စာချုပ်သတ်မှတ်ချက်၊ အစားထိုး supplier၊ backup၊ network ခွဲစိတ်မှုနှင့် incident တုံ့ပြန်ရေးတို့ကို အန္တရာယ်အလိုက် ရွေးချယ်ပါ။

Monitor — ဆက်လက်စောင့်ကြည့်ခြင်း

Supplier၊ ထုတ်ကုန်၊ ပိုင်ဆိုင်မှု၊ software update၊ အားနည်းချက်နှင့် ခြိမ်းခြောက်မှုအခြေအနေများ ပြောင်းလဲနိုင်သည်။ သတ်မှတ်ကာလအလိုက် ပြန်လည်စစ်ဆေးခြင်း၊ သတင်းပို့ချက်လက်ခံခြင်း၊ supplier အပြောင်းအလဲကို စောင့်ကြည့်ခြင်းနှင့် ထိန်းချုပ်မှု အလုပ်လုပ်နေမှုကို တိုင်းတာခြင်း လိုအပ်သည်။

၅။ ဝယ်ယူရေးနှင့် supplier ဆက်ဆံရေး

လုံခြုံရေးကို ပစ္စည်းဝယ်ယူခြင်းမှ ထည့်သွင်းစားပါက ပြုဆင်စရိတ်များပိုမြင့်တက်လာနိုင်သည့်အပြင် လုံခြုံရေးလုံခြုံမှုအစကတည်းက လုံခြုံရေးလိုအပ်ချက်၊ ထုတ်ကုန်၏ မူလရင်းမြစ်၊ update ပံ့ပိုးမည့်ကာလ၊ အားနည်းချက်တင်ပြမှု၊ incident အကင်းကင်းခြင်းနှင့် ဝန်ဆောင်မှုရပ်ဆိုင်းခြင်းတို့ကို သတ်မှတ်ပါ။

- **Supplier** ရွေးချယ်မှု လုပ်ငန်းမှတ်တမ်း၊ နည်းပညာအရည်အသွေး၊ လုံခြုံရေးလုပ်ထုံးလုပ်နည်းနှင့် အောက်ဆင့်ပေးသွင်းသူစီမံပုံကို သင့်တော်သလို စစ်ဆေးပါ။
- စာချုပ်တွင် လုံခြုံရေးလိုအပ်ချက်၊ အားနည်းချက်ဖော်ထုတ်/အသိပေးမှု၊ patch နှင့် support ကာလ၊ log နှင့် သက်သေအထောက်အထားပေးမှု၊ incident ပူးပေါင်းဆောင်ရွက်မှုတို့ကို ရှင်းလင်းရေးသားပါ။
- လိုအပ်သည့်အခါ software component စာရင်း (ဥပမာ **SBOM**)၊ ထုတ်ကုန်အရင်းအမြစ်နှင့် build/update လုပ်ငန်းစဉ်အကြောင်း အချက်အလက်တောင်းခံပါ။ အချက်အလက်ရရှိခြင်းတစ်ခုတည်းက လုံခြုံခြင်းအာမခံချက်မဟုတ်ပါ။
- စာချုပ်သက်တမ်းကုန်ဆုံးချိန်၊ supplier ပြောင်းချိန်နှင့် ပစ္စည်းပစ္စိုက်/ဖျက်သိမ်းချိန်တွင် account ပိတ်ခြင်း၊ data ပြန်လည်ရယူခြင်း/ဖျက်ခြင်းနှင့် အစားထိုးအစီအစဉ်ကို စီမံပါ။

၆။ ဖြစ်နိုင်သည့် ခြိမ်းခြောက်မှုနှင့် အားနည်းချက်များ

- အတု သို့မဟုတ် မူလရင်းမြစ်မသေသော hardware/အစိတ်အပိုင်း ဝင်ရောက်လာခြင်း။
- ဆော့ဖ်ဝဲအတွင်း မလိုလားအပ်သော code သို့မဟုတ် နောက်တံခါး (backdoor) ထည့်သွင်းခြင်း။
- အားနည်းချက်ပါသော library၊ firmware၊ operating system သို့မဟုတ် ပြုသုံးထားသော component ကြောင့် စနစ်တစ်ခုလုံး ထိခိုက်ခြင်း။
- **Supplier** ၏ account၊ build pipeline၊ update server သို့မဟုတ် ပြုပြင်ဆင်ဆင်မှုကို တိုက်ခိုက်သည့်က သိမ်းပိုက်ခြင်း။
- ထုတ်လုပ်မှု၊ ဖွံ့ဖြိုးမှု၊ ပြုဆင်မှုနှင့် maintenance လုပ်ငန်းစဉ်တွင် မလုံခြုံစွာ စီမံခန့်ခွဲမှု၊ မတော်တဆ အားပေးမှု ဖြစ်ခြင်း။

- ပထဝီနိုင်ငံရေး၊ ဥပဒေ၊ ပိုင်ဆိုင်မှုပိုင်ခွင့်လဲမှ၊ သို့မဟုတ် **supplier** တစ်ဦးတည်းအပေါ် မူတည်မှုကင်းရှင်း ဝန်ဆောင်မှုရပ်တန့်ခြင်း သို့မဟုတ် ထိန်းချုပ်မှုဆုံးရှုံးခြင်း။

၇။ အရေးကြီးသော အဆင်မပြေမှုအချက်များ

- ခေါင်းဆောင်ပိုင်းက ပိုင်ဆိုင်မှု၊ တာဝန်နှင့် ဘတ်ဂျက်ကို သတ်မှတ်ပေးအပ်ရန်အတွက် လုပ်ငန်းဆုံးဖြတ်ချက်များနှင့် ချိတ်ဆက်ထားခြင်း။
- ပစ္စည်းနှင့် **supplier** များစာရင်းကို ထိန်းသိမ်းပေးအပ်မှုအလျက် ဦးစားပေးထားခြင်း။
- ဝယ်ယူရေး၊ စနစ်တည်ဆောက်ရေး၊ လုံခြုံရေး၊ ဥပဒေရေးရာနှင့် လုပ်ငန်းပိုင်ရှင်များ အစောပိုင်းကတည်းက ပူးပေါင်းခြင်း။
- **C-SCRM** မူဝါဒနှင့် အစီအစဉ်များကို လုပ်ဆောင်နိုင်သော တာဝန်၊ အချိန်၊ အထောက်အထားနှင့် တိုင်းတာချက်များအဖွဲ့ ပြောင်းလဲခြင်း။
- အရေးကြီး **supplier** များ၏ အပြောင်းအလဲ၊ **incident**၊ အားနည်းချက်နှင့် စွမ်းဆောင်ရည်ကို ဆက်တိုက်စောင့်ကြည့်ခြင်း။

၈။ လက်တွေ့စတင်ရန် စစ်ဆေးစာရင်း

- အရေးကြီးဆုံး IT/OT စနစ်၊ **data** နှင့် ဝန်ဆောင်မှု ၁၀ ခုကို စာရင်းပစ်ပါ။
- စနစ်တစ်ခုစီအတွက် ပိုင်ရှင်၊ **supplier**၊ အောက်ဆင့် **supplier** သိရှိနိုင်မှု၊ အရေးပါမှုနှင့် အစားထိုးရလွယ်ကူမှုကို မှတ်တမ်းတင်ပါ။
- အရေးကြီးမြေပြင်သော **supplier** များအတွက် လုံခြုံရေးစစ်ဆေးမေးခွန်း၊ လက်ခံနိုင်သောသက်သေ၊ ဆက်သွယ်ရမည့်တာဝန်ခံနှင့် ပြန်လည်သုံးသပ်မည့်ကာလ သတ်မှတ်ပါ။
- ဝယ်ယူမှုအသစ်များတွင် **update** ကာလ၊ **vulnerability disclosure**၊ **incident notice**၊ **access control** နှင့် **service exit** ကို စာချုပ်ထဲ ထည့်ပါ။
- **Supplier** သို့မဟုတ် **update** တစ်ခု ထိခိုက်သွားပါက ပိတ်ဆို့၊ အစားထိုး၊ **backup** မှပူလုပ်ပါ။ အသုံးပြုအသိပေးမည့် အစီအစဉ်ကို စမ်းသပ်ထားပါ။
- အန္တရာယ်လျော့ချမှု အလုပ်ဖွဲ့/မဖွဲ့ကို စာရင်းပည့်စုံမှု၊ အားနည်းချက်ပင်ဆင်ချိန်၊ **supplier incident** တုံ့ပြန်ချိန်နှင့် **contingency** စမ်းသပ်မှုတို့ဖွင့်တိုင်းတာပါ။

၉။ မူရင်း NIST စာတမ်း၏ ဖွဲ့စည်းပုံ

မူရင်းတွင် **C-SCRM** ကို အဖွဲ့အစည်းတစ်ခုလုံး၏ **risk management** ထဲ ပေါင်းစည်းပုံ၊ အဆင်မပြေမှုအတွက် အရေးကြီးသည့်အချက်များနှင့် **control** များ ပါဝင်သည်။ ထို့အပြင် **risk scenario** များ၊ **C-SCRM** မူဝါဒ/အစီအစဉ်/

အန္တရာယ်အကဲဖြတ်မှုအတွက် **template** များ၊ လုပ်ငန်းအဆင့်လိုက် **risk management** စက်ဝန်းနှင့် **glossary** တို့ပါဝင်သည်။

နမူနာ **scenario** များတွင် **supplier** အပေါ် ပဋိပက္ခအစိုးရ၏ သစ္စာ၊ ဆက်သွယ်ရေးပစ္စည်းအတွက် စက်မှုလုပ်ငန်းဆိုင်ရာ လျှို့ဝှက်ချက်ခိုးယူမှု၊ **malicious code** ထည့်သွင်းမှု၊ မတော်တဆပေါက်ကွဲမှုနှင့် အားနည်းသော **component** ကို စနစ်များအတွင်း ပြန်သုံးမှုတို့ကို ဆွေးနွေးထားသည်။

၁၀။ ဝေါဟာရတိုများ

- **C-SCRM — Cybersecurity Supply Chain Risk Management:** ဆိုက်ဘာလုံခြုံရေးပစ္စည်း/ဝန်ဆောင်မှု ကွင်းဆက်အန္တရာယ်စီမံမှု။
- **ICT — Information and Communications Technology:** သတင်းအချက်အလက်နှင့် ဆက်သွယ်ရေးနည်းပညာ။
- **OT — Operational Technology:** စက်မှု၊ အဆောက်အအုံနှင့် လုပ်ငန်းစက်ပစ္စည်းများကို စောင့်ကြည့်/ထိန်းချုပ်သည့် နည်းပညာ။
- **SBOM — Software Bill of Materials:** ဆော့ဖ်ဝဲတစ်ခုတွင် ပါဝင်သော **component** များစာရင်း။
- **Risk appetite —** အဖွဲ့အစည်းတစ်ခုက ရည်မှန်းချက်အတွက် လက်ခံနိုင်မည့် အန္တရာယ်အမျိုးအစားနှင့် ပမာဏ။
- **Risk tolerance —** သတ်မှတ်ထားသော ရည်မှန်းချက် သို့မဟုတ် အန္တရာယ်တစ်ခုအတွက် လက်ခံနိုင်သည့် ကွာဟမှု/ကန့်သတ်ချက်။

ကိုးကားရင်းမြစ်နှင့် အသုံးပြုမှုမှတ်ချက်

အခြေခံရင်းမြစ် — Jon Boyens နှင့် အဖွဲ့၊ **Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations, NIST Special Publication 800-161 Rev. 1 Update 1**, ၂၀၂၂ (၂၀၂၄-၁၁-၀၁ အထိ ပြင်ဆင်ချက်များပါဝင်သည်)။ DOI: <https://doi.org/10.6028/NIST.SP.800-161r1-upd1>

ဤမူကြမ်းစာတမ်းသည် NIST မူရင်းစာတမ်း၏ အယူအဆများကို ဖတ်ရှုရလွယ်ကူစေရန် ပြန်လည်စီစဉ်ထားသည့် လေ့လာရေးအကျဉ်းချုပ်ဖြစ်သည်။ တရားဝင်လိုက်နာရမည့် ထိန်းချုပ်ချက်များ၊ နည်းပညာသတ်မှတ်ချက်များနှင့် ပုံစံဇယားများအတွက် မူရင်း PDF ကို ကြည့်ပါ။

