“Kiberxavfsizlik hodisalariga chora ko‘rish” (CERT/CSIRT) xizmatini tashkil etish to‘g‘risida ko‘rsatmalar

Kiberxavfsizlik hodisalariga chora ko‘rish jamoasi/xizmati (*CERT/*CSIRT) – axborot xavfsizligi hodisalari yoki tahdidlariga tezkor chora ko‘rish vazifasini bajaruvchi axborot texnologiyalari (AT) xavfsizligi mutaxassislaridan iborat jamoa bo‘lib, ular ushbu turdagi hodisa va tahdidlarni aniqlash, ularni boshqarish, tasniflash, oldini olish shuningdek, o‘z vakolatiga kiruvchi kibermakonda yuzaga kelgan kiberxavfsizlik hodisalar oqibatlarini bartaraf etish bilan shug‘ullanadilar.

CERT/CSIRT jamoasini tashkil etishda quyidagi **7 ta** elementni inobatga olish muhim hisoblanadi:

1. **Tashkiliy tuzilma (Organizational structure)** – ushbu element ba’zida Homiylik yoki Affilatsiya deb ham yuritiladi. CSIRTning tashkiliy tuzilmaga ega bo‘lishi muhim hisoblanib, bunda jamoaning tashkilotdagi o‘rni, undan yuqori turuvchi tashkilot yoki vakolat doirasidagi pozitsiyasini ko‘rsatadi. Aksar milliy CERT/CSIRT jamoalari davlat tashkilotlarida tarkibida faoliyat yuritadi, sohaviy jamoalar esa tijorat va xususiy sektor korxonalari, tadqiqot institutlari yoki ta’lim muassasalari bilan bog‘liq bo‘lishi mumkin.

2. **Doimiylik (Availability) –** CERT/CSIRT xizmatlarining doimiyligi yoki mavjudliligi asosan undan yuqori turuvchi tashkilotning ish soatlariga bog‘liq bo‘ladi. Agar CERT/CSIRT 24/7 rejimida ishlamasa, ish vaqtidan tashqari hodisalardan xabardor bo‘lish uchun shart sharoitlar yaratishi kerak. Odatda jamoa a’zolaridan biri ish soatlaridan tashqari navbatchi bo‘lib, kommunikatsiya kanallari (elektron pochta, telefon va h.k.) orqali kelayotgan hisobotlar va hodisalar to‘g‘risidagi xabarlarni kuzatib borishi va muhimlilik darajasidan kelib chiqib darhol yoki ish soatlarida choralar ko‘rilishini hal qiladi. Shuningdek, sohaviy CERT/CSIRT xizmatlarining mavjudligini belgilashda tashkilotning ish muhitini hisobga olish muhim. Masalan, agar AKT bo‘limi faqat ish soatlarida muammolarni hal qilsa, CERT/CSIRT xizmatlarini 24/7 rejimida ishlatish samarali bo‘lmasligi mumkin, chunki muammolar odatda AKT bo‘limlari mutaxassislari bilan birgalikda bartaraf etiladi.

3. **Asosiy xizmatlar (Core services) –** CERT/CSIRT jamoalari o‘z maqsad vazifalari, missiyasi hamda yuklatilgan majburiyatlaridan kelib chiqib turli xil xizmatlarni taklif etishi mumkin. Asosiy xizmatlarga misol qilib: hodisalarga chora ko‘rish berish; kibertahdidlarni monitoring qilish va aniqlash; xavfsizlik bo‘yicha konsultatsiyalar; Kiberhodisalarni tekshirish va raqamli kriminalistika; boshqalar.

4. **Tarkibiy tuzilma (Staffing requirements)** – xodimlarining malakalari CSIRT jamoasining samarali faoliyat yuritishida muhim rol o‘ynaydi. Har bir jamoa taklif qilinayotgan xizmatlar hamda o‘z vakolatiga kiruvchi kibermakon muhitidan kelib chiqib hodimlar sonini hamda yuklatilgan vazifalaridan kelib chiqib ulardan ma’lum bilim va ko‘nikmalar talab qiladi. Misol tariqasida, 2 ta xizmatni taklif etish uchun eng kamida 4 ta mutaxassis to‘liq ish grafigida talab qilinadi. 24/7 rejimida faoliyat olib boruvchi CERT/CSIRT jamoasiga eng kamida 12 ta mutaxassis talab etiladi.

5. **Infratuzilma va vositalar (Infrastructure and tooling)** – CERT/CSIRT xizmati foydalanadigan axborot infratuzilmalari va telekommunikatsiya tarmoqlari nafaqat CERT/CSIRT tomonidan to‘plangan maxfiy ma’lumotlarni himoya qilish, balki jamoa faoliyati kiberxavfsizlik holatini ham inobatga olgan holda, e’tibor bilan loyihalashtirilishi kerak. Axborot saqlovchi infratuzilmalar va xodimlar ish joylari talablarga muvofiq ravishda qurilishi va himoya qilinishi lozim.

6. **Tashqi va ichki aloqalar (Internal and external relationships)** – CERT/CSIRT jamoasi o‘zi faoliyat olib borayotgan ish muhitida boshqa bo‘lim va ulushdorlar (stakeholder) bilan davomiy hamkorlikda bo‘lishi muhim hisoblanib, kiberhodisalar yuz berganda ularga tezkor va samarali chora ko‘rishni ta’minlaydi. CERT/CSIRT jamoalari asosan AKT bo‘limi, tarmoq administratorlari, ichki jismoniy xavfsizlik bo‘limi, yuridik byuro va hodimlarni boshqarish bo‘limlari bilan yaqin hamkorlikda ishlashi muhim sanaladi. Shuningdek, tashqi aloqalarga, xalqaro va mahalliy CERT/CSIRT jamoalari, kiberxavfsizlik sohasidagi tashkilotlar hamda Milliy CERT/CSIRT xizmatlari bilan uzluksiz hamkorlik zarur sanaladi.

7. **Moliyalashtirish modeli (Funding model)** – Uzoq muddatli barqarorlikni ta’minlashda CERT/CSIRT jamoasining faoliyatini moliyalashtirish modeli muhim hisoblanadi. Moliyalashtirish o‘z ichiga CERT/CSIRT xizmatini tashkil etish uchun sarflanadigan dastlabki sarmoya, shuningdek, xodimlar, infratuzilma, inshootlar, dasturiy ta’minot litsenziyalari va boshqa operatsion xarajatlarni o‘z ichiga olishi lozim.

CERT/CSIRT jamoasi faoliyati rivojlanish (yetuklik) darajasini tekshirish uchun FIRST hamda NCA tashkilotlari tomonidan ishlab chiqilgan SIM3 **(Security Incident Management Maturity Model “https://sim3-check.opencsirt.org”)** modelidan foydalanish tavsiya etiladi.