Advisory

१) असम्बन्धित तथा अपरिचित व्यक्ति तथा संस्थाबाट आएका Email हरु Phishing तथा Spam email हुन सक्ने हुँदा त्यसको आधिकारिकता पुष्टि नभएसम्म नखोल्ने। साथै यस सम्वन्धमा आफ्ना कर्मचारीहरु तथा सरोकारवालाहरुलाई समेत सजग गराउने।

२) आफ्नो निकायमा प्रयोग भईरहेका सूचना प्रविधि प्रणाली, Email लगायतका अन्य प्रणालीहरुमा सम्भव भएसम्म Multi-factor Authentication को प्रयोग गर्ने।

३) पासवर्ड राख्दा सहजै अनुमान गर्न नसकिने गरी सुरक्षित Password (Non-Trivial Password Policy अनुसार) राख्ने ।

४) प्रयोगमा रहेका Anti-virus, Database, Application Libraries, Operating System, Network devices, Security devices, Servers आदिलाई नियमित रुपमा अद्यावधिक गर्ने।

५) सूचना प्रविधि प्रणालीहरुको विकास तथा प्रयोग गर्दा "नेपाल सरकारको सूचना प्रविधि प्रणाली (व्यवस्थापन तथा सञ्चालन) निर्देशिका, २०७१" ले तोकेका Government Enterprise Architecture (GEA) सम्वन्धी मापदण्डहरू पालना गर्ने।

६) नयाँ सूचना प्रविधि प्रणालीहरूको विकास गरी Live गर्नु अघि अनिवार्य रूपमा Vulnerability Assessment and Penetration Testing (VAPT) लगायतका सुरक्षा परीक्षण गर्ने।

७) सरकारी निकायहरूले विकास गरेका वा गर्न लगाइएका सूचना प्रविधि प्रणालीको Source Code सुरक्षित राखी अद्यावधिक गर्ने व्यवस्था मिलाउने।

८) आ-आफ्नो निकायमा प्रयोग भईरहेका सूचना प्रविधि प्रणालीहरुको कम्तीमा पनि वर्षको एक पटक अनिवार्य रूपमा VAPT लगायतका सूरक्षा जाँच (Security Audit) गर्ने व्यवस्था मिलाउने।

<u>नोट</u>: *सरकारी निकायहरुले* VAPT *का लागि सूचना प्रविधि विभागबाट सहयोग लिन सक्नेछन्।*

९) Application हरुमा SSL को प्रयोग गर्ने।

१०) Genuine License भएका hardware तथा software हरू मात्र प्रयोग गर्ने।

११) आफ्नो संस्थाको Business Continuity Plan तयार गरी लागु गर्ने। साथै डाटाको नियमित रूपमा Backup तथा Archive गरी सुरक्षित राख्ने।

१२) डाटाको Unauthorized प्रयोग हुन नदिन आफ्नो संस्थामा डाटा Encryption को व्यवस्था गर्ने।

१३) संस्थामा कार्यरत कर्मचारीहरुलाई साइवर सुरक्षासम्बन्धी नियम-निर्देशनहरू, थ्रेट्स, रिस्क र समाधानका बारेमा नियमित प्रशिक्षण दिने।

१४) संस्थाले सूचना प्रविधिको प्रयोगमा आवश्यक Privacy Policy तथा Terms and Conditions निर्धारण गरी पालना गर्न निर्देशन दिने।

१५) संस्थाले कर्मचारीहरूलाई Personal डिभाइसहरूमा आधिकारिक डाटा संग्रह गर्ने, share गर्ने वा प्रसारण गर्ने जस्ता कार्यलाई निरुत्साहित गर्ने।

१६) संस्थामा नरहेका वा छाडेका व्यक्ति/कर्मचारीको प्रयोगकर्ता खाताहरू (User Accounts) निष्कृय बनाउने। लामो समयसम्म प्रयोग नभएका प्रयोगकर्ता खाताहरूलाई Deactivate गर्ने तथा खाता चालू गर्न अनुरोध आएमा मात्र Activate गर्ने ।

१७) साइवर सुरक्षाका उपकरणहरू (जस्तै Firewall, WAF, IPS/IDS) को प्रयोग गर्दा तिनिहरूको उचित Configuration तथा Security Harden गरी मात्र प्रयोग गर्ने।

१८) नेटवर्कमा विशेष सुरक्षा सम्पादन गर्नका लागि Intrusion Detection/Prevention Systems (IDS/IPS) हरु प्रयोग गर्ने।

१९) Firewall मा Inbound र Outbound Rules हरु प्रयोग गरी कार्यालयभित्रको नेटवर्कलाई सुरक्षित बनाउने। साथै अनावश्यक Port हरु बन्द गर्ने, SSH/Telnet/RDP जस्ता Remote-Access Port हरुमा Brute-force आक्रमण जोगाउन max-failed-tries-within-time-limit परिभाषित गर्ने, आवश्यकता अनुसार IP Blacklisting / IP Whitelisting गर्ने, Port-Knocking को व्यवस्था गर्ने।

२०) वायरलेस नेटवर्कलाई आन्तरिक नेटवर्कबाट अलग गर्ने व्यवस्था मिलाउने। संस्थाका Application हरू LAN बाट मात्र पहुँच योग्य बनाउने। Wi-Fi को प्रयोगलाई निरुत्साहित गर्ने तथा यसको प्रयोग Internet उपयोगको लागि मात्र गर्ने व्यवस्था मिलाउने।

२१) कार्यालयको Email ठेगाना व्यक्तिगत प्रयोजनको लागि प्रयोग नगर्ने।

२२) कुनै पनि सूचना प्रविधि सम्बन्धी उपकरणहरु मर्मतको लागि पठाउँदा सूचना चुहावट हुन सक्ने भएकाले डाटामा पहुँच नहुनेगरी (बिना Hard disk, अन्य storage, memory) मर्मतको लागि पठाउने ।

२३) सूचना प्रविधि सम्बन्धी उपकरणहरुको लिलामि गर्दा Hard disk, Storage, Memory झिकेर मात्र लिलाम गर्ने। साथै उक्त Hard disk, अन्य Storage, Memory लाई भौतिक रुपमा पूर्ण नष्ट गर्ने ।

२४) साइबर आक्रमणका कुनै घटना घटेमा वा कुनै शंकास्पद ईमेल/लिंक/फाइलहरु ईमेल मार्फत् प्राप्त भएमा सोको जानकारी राष्ट्रिय सूचना प्रविधि आकस्मिक सहायता समूहको आधिकारिक वेबसाइट https://nitert.gov.np मा गई रिपोर्ट गर्न सकिने।

Anil Kumar Dutta

Digitally signed by Anil Kumar Dutta
Date: 2023.07.07 14:14:50 +05'45'