৫০১১৯

বাংলাদেশ ব্যাংক
(সেন্ট্রাল ব্যাংক অব বাংলাদেশ)
প্রধান কার্যালয়
মতিঝিল, ঢাকা-১০০০
বাংলাদেশ।

সাইবার সিকিউরিটি ইউনিট

সূত্র নং-সিএসইউ/ইন্সিডেন্ট/১০(৪)/২০২৩-

তারিখ: ০২/০৮/২০২৩ ইং

ব্যবস্থাপনা পরিচালক/প্রধান নির্বাহী কর্মকর্তা
বাংলাদেশে কার্যরত সকল তফসিলি ব্যাংক ও আর্থিক প্রতিষ্ঠান।

মহোদয়,

বিষয়: বাংলাদেশে কার্যরত সকল ব্যাংক ও আর্থিক প্রতিষ্ঠানের সাইবার নিরাপত্তা জোরদারকরণ প্রসঙ্গে।

সাম্প্রতিক সাইবার হামলা বৃদ্ধি বিবেচনায় বাংলাদেশের যেকোন ব্যাংক ও আর্থিক প্রতিষ্ঠানে সাইবার হামলা হওয়ার আশংকা রয়েছে। এরূপ যে কোন সাইবার আক্রমণ মোকাবেলায় সকল ব্যাংক ও আর্থিক প্রতিষ্ঠানের জন্য নিম্নলিখিত ব্যবস্থা গ্রহণ করা অতীব জরুরী:

ক) সাইবার আক্রমণের শিকার হলে ডিজিটাল সিকিউরিটি এজেন্সি (ডিএসএ), বিজিডি ই-গভ সার্ট এবং বাংলাদেশ ব্যাংককে বিষয়টি তৎক্ষণাৎ অবহিত করা;

খ) বাংলাদেশ ব্যাংক কর্তৃক প্রণীত আইসিটি গাইডলাইন-২০২৩ পূর্ণাঙ্গরূপে অনুসরণ করে নিম্নের বিষয়সমূহ বিশেষভাবে পরিপালন করা:

i. Least Priviledged Principle অনুসরণ করে Access Rules বাস্তবায়ন এবং সকল সিস্টেমের Privileged User (Admin/Root) সমূহের পাসওয়ার্ড অতি দ্রুত পরিবর্তন করার ব্যবস্থা গ্রহণ করার পাশাপাশি অপ্রয়োজনীয় ইউজারসমূহ Disable করা;
ii. ব্যাংকের ইন্টারনেট সংযোগ সীমিত করা এবং এই সীমিত ইন্টারনেট সংযোগে Anti Advanced Persistent Threat (APT) সম্বলিত Secure Web Gateway-ব্যবহার করা;
iii. ইমেইল সার্ভারসমূহের জন্য Anti APT সম্বলিত Secure Email Gateway ব্যবহার করা;
iv. সকল সার্ভার এবং End User-এ Endpoint Detection and Response (EDR) (Sandboxingসহ) সল্যুশন ব্যবহার নিশ্চিত করা;
v. সকল হার্ডওয়্যার (সার্ভার, নেটওয়ার্ক, সিকিউরিটি ডিভাইস ইত্যাদি) ও সফটওয়্যারসমূহের (Operating System, Database ও সকল এপ্লিকেশন), এবং End User Device সমূহের Patch হালনাগাদ করা। স্বয়ংক্রিয়ভাবে Patch আপডেট করার বিষয়ে প্রয়োজনীয় পদক্ষেপ গ্রহণ করা;
vi. স্বয়ংক্রিয় টেপ ব্যাকআপ সিস্টেমের মাধ্যমে নিয়মিতভাবে চলমান সকল এপ্লিকেশন এবং ডাটাবেজ এর ব্যাকআপ সংরক্ষণ করা এবং টারশিয়ারি (3^{rd}) ব্যাকআপ নিশ্চিত করা;
vii. Disaster Recovery Site (DRS) অবশ্যই Operational এবং Tested হওয়া;
viii. সকল পর্যায়ের কর্মকর্তাদের সাম্প্রতিক সাইবার ঝুঁকি ও করণীয় সম্পর্কে সচেতনতা কার্যক্রম গ্রহণ করা;

চলমান পাতা -০২

ফোন ঃ ৮৮-০২-৯৫৫০৪৪৮, ৯৫৫৪৮৯৬, আইপি ঃ ৮৮-০২-৫৫৬৬৫০০১-৬, ফ্যাক্স ঃ ৮৮-০২-৯৫৩০৪৭৯, www.bb.org.bd

(পূর্ববর্তী পৃষ্ঠার পর)

ix. অননুমোদিত পোর্টেবল ডিভাইস (ইউএসবি সহ অন্যান্য) নিয়ন্ত্রণের জন্য প্রয়োজনীয় পদক্ষেপ গ্রহণ করা;

x. ডাটার সুরক্ষার জন্য প্রয়োজনীয় পদক্ষেপ গ্রহণ করা (যেমনঃ Encryption, Access Controls বাস্তবায়ন);

xi. Third Party/Vendor/Partners সংশ্লিষ্ট ঝুঁকি ব্যবস্থাপনার ক্ষেত্রে কার্যকরী পদক্ষেপ গ্রহণ করা;

xii. Vulnerability Assessment and Penetration Testing (VAPT) কার্যক্রমের মাধ্যমে যেসকল সিস্টেমে দুর্বলতা ইতোমধ্যে চিহ্নিত হয়েছে সেই দুর্বলতাসমূহ অতি দ্রুততার সাথে নিরসন করা এবং পরবর্তী VA কার্যক্রমের মাধ্যমে Follow-up নিশ্চিত করা;

xiii. যে সকল Device এর End of Life (EOL)/End of Support (EOS) ইতোমধ্যে অতিক্রান্ত হয়েছে, সেগুলোর তালিকা প্রণয়নপূর্বক প্রযোজ্য ক্ষেত্রে License/Contract নবায়ন করা, Service Level Agreement (SLA) নবায়ন করা, অন্যথায় নতুন ক্রয়ের উদ্যোগ গ্রহণ করা;

xiv. সকল নেটওয়ার্ক ট্রাফিক (অভ্যন্তরীণ এবং বাহির থেকে আগত) ২৪/৭ ভিত্তিতে মনিটরিং করা এবং কার্যকর Network Operations Center (NOC) এবং Security Operations Center (SOC) স্থাপন করা;

xv. Industry best practices, Standards এবং সরকারের আইন/গাইডলাইন/নীতিমালার সাথে সামঞ্জস্য রেখে Data Center (DC), Near Data Center (NDC), Far Data Center (FDC)/DRS পূর্ণাঙ্গভাবে চালু করা;

এমতাবস্থায়, উল্লিখিত বিষয়ে জরুরী ভিত্তিতে প্রয়োজনীয় ব্যবস্থা গ্রহণপূর্বক গৃহীত পদক্ষেপের হালনাগাদকৃত তথ্য (হার্ডকপি) চীফ ইনফরমেশন সিকিউরিটি অফিসার, বাংলাদেশ ব্যাংক, প্রধান কার্যালয়, ঢাকা বরাবর এবং ciso.csu@bb.org.bd ইমেইল মারফত (সফটকপি) আগামী ৩০/০৮/২০২৩ইং তারিখের মধ্যে প্রেরণের জন্য আপনাদের অনুরোধ করা হলো।

ধন্যবাদান্তে

(মোহাম্মদ ইমতিয়াজ কবির)
ডেপুটি চীফ ইনফরমেশন সিকিউরিটি অফিসার
সাইবার সিকিউরিটি ইউনিট, বাংলাদেশ ব্যাংক, প্রধান কার্যালয়, ঢাকা
মোবাইলঃ ০১৭৩০০২৮৬৮৩
ইমেইলঃ imtiaz.kabir@bb.org.bd