রাজশাহী কৃষি উন্নয়ন ব্যাংক

প্রধান কার্যালয়, রাজশাহী

তথ্য ও যোগাযোগ প্রযুক্তি বিভাগ

ফোন: ০৭২১-৮৬২৪৫৪
ফ্যাক্স: ০৭২১-৮৬২৪৫৬
ই-মেইল: dgmict@rakub.org.bd

সার্কুলার লেটার নং আইসিটিবি-০৫/২০১৭ তারিখ: ০৭-০৮-২০১৭

বিষয়: WannaCry র‍্যানসমওয়্যার ও করণীয় প্রসঙ্গে।

সূত্র-১: আর্থিক প্রতিষ্ঠান বিভাগের স্মারক নং: ৫৩.০০.০০০০.২০১.৯৯.০০১.১৭/৩২ তারিখ: ২১-০৫-২০১৭।
সূত্র-২: ডাক ও টেলিযোগাযোগ বিভাগের স্মারক নং: ১৪.০০.০০০০.০১০.০২২.২৫.১৩-২২৮ তারিখ: ১৭-০৫-২০১৭।

বর্তমানে বিশ্বের অনেক দেশে WannaCry র‍্যানসমওয়্যার (ভাইরাসধর্মী সফটওয়্যার) দ্বারা আক্রমণের শিকার হচ্ছে। এক্ষেত্রে সাইবার আক্রমণের ঝুঁকিতে বাংলাদেশও রয়েছে। সাধারণত কম্পিউটার ব্যবহারকারী যদি কোন স্প্যাম ই-মেইল থেকে কোন সন্দেহজনক ইউআরএল (URL) অথবা সন্দেহজনক Attachment ডকুমেন্ট এ ক্লিক করে, যা WannaCry র‍্যানসমওয়্যার যুক্ত, সেটি সাথে সাথে ঐ কম্পিউটার ব্যবহারকারীর সব তথ্য এনক্রিপ্ট/লক করে ফেলে এবং সেই তথ্য আগের অবস্থায় ফিরে পাবার জন্য মুক্তিপণ দাবি করে। WannaCry ম্যালওয়্যারটি নেটওয়ার্ক এ যুক্ত অন্য উইন্ডোজ সিস্টেম স্ক্যান করে এবং যে সিস্টেমে MS17-010 প্যাচ দেয়া নেই সেই সিস্টেমটিকেও সংক্রমিত করে।

০২। উপর্যুক্ত বিষয় ও সূত্রোক্ত পত্রের মাধ্যমে জানানো যাচ্ছে যে, WannaCry র‍্যানসমওয়্যার কিভাবে নেটওয়ার্কে আক্রমণ করে এবং কি উপায়ে উক্ত র‍্যানসমওয়্যার হতে নিরাপদ থাকা যাবে সে বিষয়ে করণীয় সম্পর্কে উল্লেখ করে পরবর্তী প্রয়োজনীয় ব্যবস্থা গ্রহণের নির্দেশ দেয়া হয়েছে।

০৩। সংশ্লিষ্ট বিষয়ে ডাক ও টেলিযোগাযোগ বিভাগ থেকে প্রাপ্ত পত্র সংশ্লিষ্ট সকলের অবগতি ও প্রয়োজনীয় ব্যবস্থা গ্রহণের জন্য অপর পৃষ্ঠায় পুনঃমুদ্রণ করে প্রেরণ করা হলো। উল্লেখ্য, WannaCry Ransomware MS17-010 প্যাচটি https://technet.microsoft.com/en-us/library/security/ms17-010.aspx লিংক থেকে ডাউনলোড করা যাবে।

০৭.০৮.১৭

(মোঃ মিজানুর রহমান)
উপ-মহাব্যবস্থাপক

প্রকা/আইসিটিবি-১৪/২০১৭-২০১৮/ ৮০ (৪৫১) তারিখ: ঐ

সদয় অবগতি ও প্রয়োজনীয় ব্যবস্থা গ্রহণের জন্য অনুলিপি প্রেরিত হলো:

০১। স্টাফ অফিসার, ব্যবস্থাপনা পরিচালক মহোদয়ের সচিবালয়, রাকাব, প্রধান কার্যালয়, রাজশাহী।
০২। স্টাফ অফিসার, উপ-ব্যবস্থাপনা পরিচালক মহোদয়ের সচিবালয়, রাকাব, প্রধান কার্যালয়, রাজশাহী।
০৩। স্টাফ অফিসার, সকল মহাব্যবস্থাপক মহোদয়ের দপ্তর, রাকাব, প্রধান কার্যালয়, রাজশাহী।
০৪। মহাব্যবস্থাপক মহোদয়ের স্টাফ অফিসার, রাকাব, বিভাগীয় কার্যালয়, রাজশাহী/রংপুর।
০৫। সকল উপ-মহাব্যবস্থাপক/সচিব/বিভাগীয় প্রধান, রাকাব, প্রধান কার্যালয়, রাজশাহী।
০৬। অধ্যক্ষ, রাকাব, প্রশিক্ষণ ইনস্টিটিউট,উপশহর, রাজশাহী।
০৭। বিভাগীয় নিরীক্ষা কর্মকর্তা, রাকাব, বিভাগীয় নিরীক্ষা কার্যালয়, রাজশাহী/রংপুর।
০৮। সকল জোনাল ব্যবস্থাপক, রাজশাহী কৃষি উন্নয়ন ব্যাংক।
০৯। প্রজেক্ট ডাইরেক্টর, এসইসিপি, রাজশাহী।
১০। উপ-মহাব্যবস্থাপক/ব্যবস্থাপক, রাকাব, ঢাকা কর্পোরেট শাখা, ঢাকা/স্থানীয় মুখ্য কার্যালয়, রাজশাহী।
১১। সকল জোনাল নিরীক্ষা কর্মকর্তা, রাজশাহী কৃষি উন্নয়ন ব্যাংক।
১২। সকল শাখা ব্যবস্থাপক, রাজশাহী কৃষি উন্নয়ন ব্যাংক।

07.08.17.

(মোঃ আবুল কালাম)
সিনিয়র মেইনটেন্যান্স ইঞ্জিনিয়ার (সমব্য)

জরুরি

গণপ্রজাতন্ত্রী বাংলাদেশ সরকার
ডাক, টেলিযোগাযোগ ও তথ্যপ্রযুক্তি মন্ত্রণালয়
ডাক ও টেলিযোগাযোগ বিভাগ
টেলিকম-১শাখা
বাংলাদেশ সচিবালয়, ঢাকা।

নথি নং- ১৪.০০.০০০০.০১০.০২২.২৫.১৩-২১৮ তারিখঃ ০৩ জৈষ্ঠ্য, ১৪২৪/১৭ মে ২০১৭ খ্রিঃ।

বিষয়ঃ WannaCry র‍্যানসমওয়্যার ও করণীয়।

বর্তমানে বিশ্বের অনেক দেশে WannaCry র‍্যানসমওয়্যার দ্বারা আক্রমণের শিকার হয়েছে। এক্ষেত্রে সাইবার আক্রমণের ঝুঁকিতে বাংলাদেশও রয়েছে। বিষয়টি নিয়ে বিগত ১৫ মে,২০১৭ তারিখে বেগম তারানা হালিম এম.পি. মাননীয় প্রতিমন্ত্রী, ডাক ও টেলিযোগাযোগ বিভাগের সভাপতিত্বে অনুষ্ঠিত সভার সিদ্ধান্ত অনুযায়ী BGD e-GOV CIRT প্রণীত নিম্নরূপ পরামর্শ অনুযায়ী ব্যবস্থা গ্রহণের জন্য নির্দেশক্রমে অনুরোধ করা হলো।

ক) WannaCry এর প্রাথমিক লক্ষ্য:
মাইক্রোসফটের অপারেটিং সিস্টেম উইন্ডোজ চালিত কম্পিউটার অ্যাটাক করা যাতে MS17-010 প্যাচ (Patch) দেয়া নেই।
খ) তাৎক্ষণিক করনীয়:
মাইক্রোসফটের অপারেটিং সিস্টেম উইন্ডোজ চালিত অনাক্রান্ত কম্পিউটার এ MS17-010 প্যাচ (Patch) দিয়ে হালনাগাদ করে নিতে হবে।
গ) WannaCry র‍্যানসমওয়্যার কিভাবে নেটওয়ার্ক এ আক্রমণ করে?
সাধারণত কম্পিউটার ব্যবহারকারী যদি কোন স্প্যাম ইমেইল থেকে কোন সন্দেহজনক ইউআরএল (URL) অথবা সন্দেহজনক Attachment ডকুমেন্ট এ ক্লিক করে, যা WannaCry র‍্যানসমওয়্যার যুক্ত, সেটি সাথে সাথে ঐ কম্পিউটার ব্যবহারকারীর সব তথ্য এনক্রিপ্ট/লক করে ফেলে এবং সেই তথ্য আগের অবস্থায় ফিরে পাবার জন্য মুক্তিপণ দাবি করে। WannaCry ম্যালওয়ারটি নেটওয়ার্ক এ যুক্ত অন্য উইন্ডোজ সিস্টেম স্ক্যান করে এবং যে সিস্টেমে MS17-010 প্যাচ দেয়া নেই সেই সিস্টেমটিকেও সংক্রমিত করে।
ঘ) নিরাপদ থাকতে যা করণীয়:
১) আপনার ডেটা রেগুলার ব্যাকআপ নিন এবং নিরাপদে অন্যকোথাও রেখে দিন।
২) উইন্ডোজ চালিত কম্পিউটার এ MS17-010 প্যাচ (Patch) দিয়ে হালনাগাদ করুন। MS17-010 সম্পর্কে বিস্তারিত জানতে BGD e-GOV CIRT এর সিকিউরিটি নিউজ বিভাগ এর লিঙ্ক এ ক্লিক করুন।
৩) রেগুলার উইন্ডোজ আপডেট করুন। এক্ষেত্রে উইন্ডোজ Automatic Update বা স্বয়ংক্রিয় হালনাগাদ চালু রাখুন।
৪) কোন untrusted online source থেকে ransomware removal tool ডাউনলোড করবেন না, এটি নতুন কোন attack করতে পারে।
৫) সর্বদা অযাচিত বা সন্দেহজনক ঠিকানা হতে আগত ই মেইল এর সোর্স যাচাই না করা পর্যন্ত সেগুলির ভিতরে থাকা লিঙ্কগুলিতে ক্লিক করা উচিত নয়।
৬) সর্বোপরি, নিশ্চিত করুন যে আপনার সিস্টেমে একটি সক্রিয় হালনাগাদ অ্যান্টি-ভাইরাস সিকিউরিটি স্যুট চালু রয়েছে এবং সবচেয়ে গুরুত্বপূর্ণভাবে, সর্বদা নিরাপত্তার সাথে ইন্টারনেট ব্রাউজ করুন।

সচিব মহোদয়ের দপ্তর, ... বিভাগ	
ডায়েরী নম্বরঃ	তারিখঃ
অতিরিক্ত সচিব AC	দ্রুত ব্যবস্থা নিন
যুগ্ম-সচিব	আলোচনা করুন
উপ-সচিব	জরুরী উপস্থাপন করুন
সিনিয়র সহকারী সচিব	নথিভুক্ত
একান্ত সচিব	
	স্বাক্ষর:

১৭/৫/১৭

(শাহানারা ইয়াসমিন লিলি)
উপসচিব
ফোনঃ ৯৫৭৪৪৪৮
telecom1@ptd.gov.bd

প্রাপক
১। সিনিয়র সচিব
মন্ত্রণালয়/ বিভাগ।
২। সচিব, তথ্য ও যোগাযোগ প্রযুক্তি বিভাগ, বাংলাদেশ সচিবালয়, ঢাকা
মন্ত্রণালয়/ বিভাগ।

Programmer