এই সময়ে সাইবার সিকিউরিটি

মইন উদ্দীন মাহ্‌মুদ

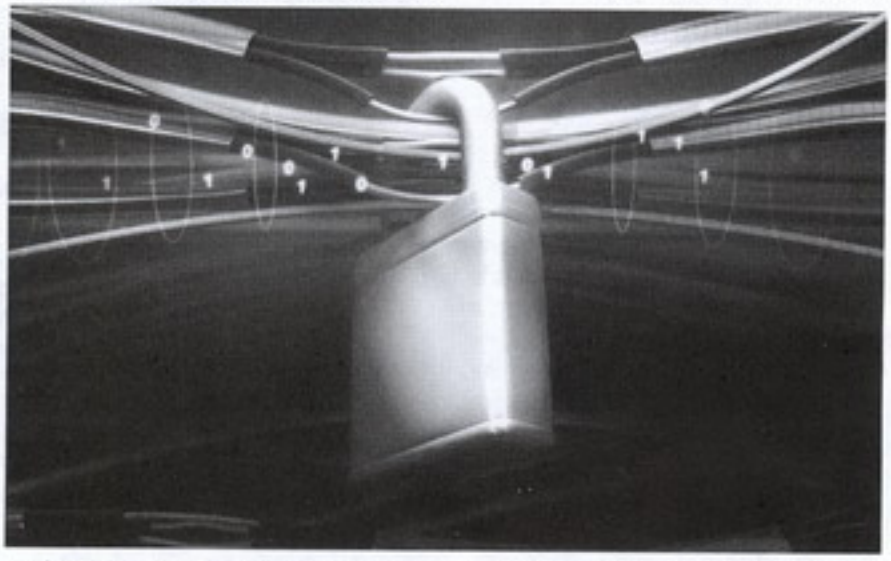
সাইবার হামলার শিকার হয়নি কখনো এমন দেশ মনে হয় একটিও খুঁজে পাওয়া যাবে না। তাই সাইবার হামলা থেকে রক্ষা পাওয়ার জন্য অর্থাৎ সাইবার হামলা প্রতিহত করার জন্য সতর্ক হয়ে উঠেছে যুক্তরাষ্ট্র, ইউরোপসহ বিশ্বের অনেক দেশ। সাইবার হামলা থেকে কিভাবে রক্ষা পাওয়া যায়, তা নিয়ে সমগ্র বিশ্ব এখন আশঙ্কিত। কেননা, ইদানীং সাইবার হামলাগুলো অতীতের যেকোনো সময়ের চেয়ে অনেক বেশি ব্যাপক ও ধ্বংসেকর।

নেটওয়ার্ক, কমপিউটার, প্রোগ্রাম এবং ডাটাকে বাইরের হামলা, ক্ষতিকর বা অনাকাঙ্ক্ষিত অ্যাক্সেস থেকে রক্ষার জন্য যে প্রযুক্তি, প্রসেস এবং প্র্যাকটিসকে ডিজাইন করা হয়, তা হলো সাইবার সিকিউরিটির বডি বা ভিত্তি। বর্তমান কমপিউটিং প্রেক্ষাপটে সিকিউরিটি পদবাচ্যটি পরোক্ষভাবে সামনে নিয়ে আসে সাইবার সিকিউরিটিকে। প্রকৃতপক্ষে আমাদের ব্যক্তিগত তথ্য বা কমপিউটারে স্টোর করা ডিজিটাল ফর্মের যেকোনো সম্পদ অথবা যেকোনো ডিজিটাল মেমরি ডিভাইসগুলোকে প্রোটেক্ট তথা নিরাপদ রাখাই হচ্ছে সাইবার সিকিউরিটি।

সাইবার সিকিউরিটির সমস্যাদায়ক উপাদানগুলোর মধ্যে অন্যতম একটি হলো সিকিউরিটির ঝুঁকির স্বভাব বা ধরন দ্রুতগতিতে এবং অবিরতভাবে বিকশিত হচ্ছে। গতানুগতিক ধারার সিকিউরিটির জন্য অ্যাপ্রোচগুলোর ফোকাস বা লক্ষ্য ছিল গুরুত্বপূর্ণ সিস্টেম কম্পোনেন্টের ওপর, যা প্রতিরোধ করতে পারে পরিচিত বড় ধরনের হুমকি। কিন্তু এতে কিছু কম গুরুত্বপূর্ণ ও অপরিহার্য সিস্টেম কম্পোনেন্ট অরক্ষিতভাবে থেকেই যায়। তাই এ ধরনের অ্যাপ্রোচ বর্তমান পরিবেশ পরিস্থিতিতে তেমন কার্যকর নয়। ফলে দিন দিন বাড়ছে তথ্যের নিরাপত্তার হুমকি। আর এ কারণে সচেতন হয়ে পড়ছেন বিশ্বের বিভিন্ন দেশের তথ্যপ্রযুক্তি সংশ্লিষ্ট শীর্ষস্থানীয় নীতি-নির্ধারক থেকে শুরু করে রাষ্ট্রনায়কেরা। সাইবার সিকিউরিটির গুরুত্ব অনুধাবন করে মার্কিন যুক্তরাষ্ট্রের প্রেসিডেন্ট বারাক ওবামা বলেন, আমাদের সাইবার নেটওয়ার্কে হামলা দিন দিন বেড়েই চলেছে। তিনি ঘোষণা দেন, সাইবার থ্রেট হলো অন্যতম প্রধান এক হুমকি, যা আমাদের জাতীয় অর্থনীতি ও নিরাপত্তাকে এখন সবচেয়ে বেশি ভয়াবহ করে তুলেছে।

সাইবার সিকিউরিটি কী?

আমাদের প্রতিদিনের জীবনের অনেক কিছুই নির্ভর করে ইন্টারনেট এবং কমপিউটারের ওপর, যেখানে সম্পৃক্ত রয়েছে কমিউনিকেশন (ই-মেইল, সেলফোন), ট্রান্সপোর্টেশন (ট্রাফিক কন্ট্রোল সিগন্যাল, উড়োজাহাজ নেভিগেশন), গভর্নমেন্ট সেক্টর (জন্ম/মৃত্যু রেকর্ড, সোশ্যাল সিকিউরিটি, লাইসেন্সিং, ট্যাক্স রেকর্ড), ফিন্যান্স (ব্যাংক অ্যাকাউন্ট, ঋণ, ইলেকট্রনিক পে-চেক), মেডিসিন (ইকুইপমেন্ট, মেডিক্যাল রেকর্ড) এবং এডুকেশন (ভার্চুয়াল ক্লাসরুম, অনলাইন রেকর্ড কার্ড, রিসার্চ) ইত্যাদি আরো অনেক কিছু। সুতরাং, কী বিশাল পরিমাণের ডাটা আপনার কমপিউটারে বা অন্য কোনো সিস্টেমে স্টোর করা আছে। যেখানে আপনার ডাটা এবং সিস্টেম স্টোর করে রাখা আছে, তা কতটুকু নিরাপদ? আর এখানেই সাইবার সিকিউরিটির বিষয়টি উঠে আসে, যেখানে প্রাধান্য পায় আমাদের প্রাত্যহিক জীবনে ব্যবহার হওয়া তথ্য ও সিস্টেমের রক্ষার বিষয়টি। তাই প্রথমেই আমাদেরকে জানতে হবে সাইবার সিকিউরিটির মূল নীতিগুলো সম্পর্কে।



সাইবার সিকিউরিটির মূল তিন নীতি হলো : ডাটার কনফিডেন্সিয়ালিটি বা গোপনীয়তা, ইন্টিগ্রিটি বা বিশুদ্ধতা এবং এভেইলিবিলিটি বা প্রাপ্যতা।

কনফিডেন্সিয়ালিটি : সংবেদনশীল বা ব্যক্তিগত তথ্যগুলোকে অবশ্যই অবিকৃত ও যথাযথভাবে ব্যক্তির কাছে শেয়ার করতে হবে।

ইন্টিগ্রিটি : তথ্যের বিশুদ্ধতা অবশ্যই ধরে রাখতে হবে এবং কোনো অবস্থাতে ডকুমেন্টের পরিবর্তন বা বিকৃতি করা যাবে না।

এভেইলিবিলিটি : তথ্য ও তথ্য ব্যবস্থাকে অবশ্যই পর্যাপ্ত হতে হবে, যাতে সবাই প্রয়োজনের সময় পায়।

সাইবার সিকিউরিটির স্ট্যান্ডার্ড

সম্প্রতি প্রতিষ্ঠা করা হয়েছে সাইবার সিকিউরিটি স্ট্যান্ডার্ড। কেননা, সংবেদনশীল বেশিরভাগ ডাটাই আজকাল নিয়মিতভাবে স্টোর করা হয় কমপিউটারে, যা ইন্টারনেটের সাথে যুক্ত। এ ছাড়া আগের সম্পাদিত অনেক কাজও ইদানীং কমপিউটারে নিয়ে আসা হচ্ছে। সুতরাং এসব কাজের নিরাপত্তার জন্য দরকার ইনফরমেশন অ্যাসুরেন্স তথা এআই এবং সিকিউরিটি। তাই আইডেন্টিটি চোরদের বিরুদ্ধে প্রতিরোধ গড়ে তুলতে সাইবার সিকিউরিটি গুরুত্বপূর্ণ। ব্যবসায় ক্ষেত্রেও সাইবার সিকিউরিটি দরকার, কেননা ব্যবসায়ীদের দরকার তাদের ব্যবসায়ের তথ্য গোপন রাখা, বিশেষ করে প্রোপাইটরি ইনফরমেশন তথা মেধাস্বত্ব তথ্য এবং প্রতিষ্ঠানের ক্লায়েন্ট ও কর্মীদের শনাক্তকরণ তথ্য।

সিকিউরিটি স্ট্যান্ডার্ড হিসেবে বর্তমানে সবচেয়ে বেশি ব্যবহার হচ্ছে আইএসও/আইইসি ২৭০০২ স্ট্যান্ডার্ড, যা চালু হয় ১৯৯৫ সালে। এই স্ট্যান্ডার্ড গঠিত হয় দু'টি মৌলিক অংশ ▸

নিয়ে। যেমন বিএস ৭৭৯৯ পার্ট-১ এবং দ্বিতীয় অংশ বিএস ৭৭৯৯ পার্ট-২। ব্রিটিশ স্ট্যান্ডার্ড ইনস্টিটিউট তথা বিএসআই এ দু'টি স্ট্যান্ডার্ড তৈরি করে। বর্তমানে এই স্ট্যান্ডার্ড আইএসও ২৭০০১ নামে পরিচিত। দি ইন্টারন্যাশনাল সোসাইটি অব অটোমেশন তথা আইএসএ ইন্ডাস্ট্রিয়াল অটোমেশন কন্ট্রোল সিস্টেম তথা আইএসিএসের জন্য ডেভেলপ করে সাইবার সিকিউরিটি স্ট্যান্ডার্ড, যা ম্যানুফ্যাকচারিং ইন্ডাস্ট্রিতে ব্যাপকভাবে প্রয়োগযোগ্য। আইএসএ ইন্ডাস্ট্রিয়াল সাইবার সিকিউরিটি স্ট্যান্ডার্ড আইএসএ-৯৯ হিসেবে পরিচিত, যা অন্যান্য ক্ষেত্রে সম্প্রসারিত হচ্ছে।

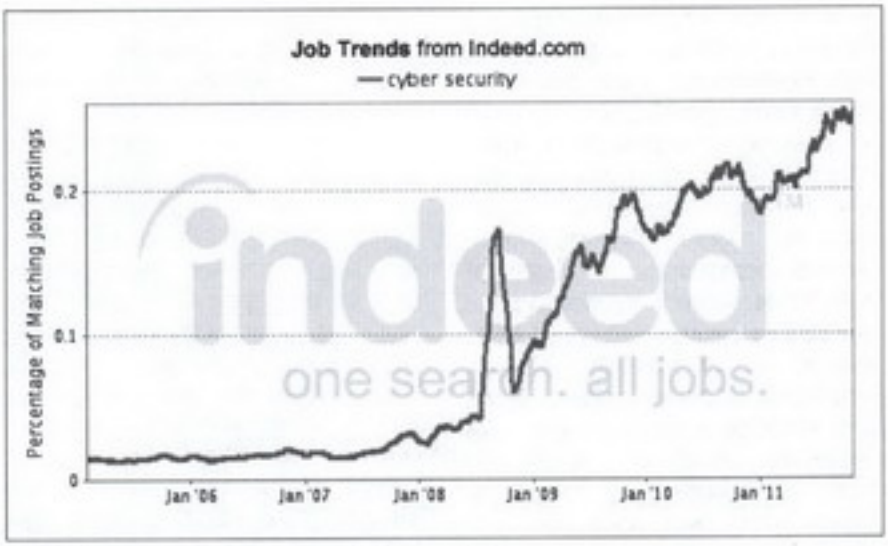
আন্তর্জাতিক পর্যায়ে কিছু উল্লেখযোগ্য সাইবার ঘটনা

২০১০ সালে আবিষ্কৃত হয় স্টাক্সনেট (Stuxnet) নামের কমপিউটার ওয়ার্ম। এটি সম্ভবত সবচেয়ে দুর্ভোগ্য সাইবার হামলাগুলোর মধ্যে অন্যতম। কোনো কোনো পর্যবেক্ষক স্টাক্সনেট হামলাকে একটি সাইবার যুদ্ধের ঘটনা মনে করেন। স্টাক্সনেটের লক্ষ্য শুধু মাইক্রোসফট উইন্ডোজভিত্তিক সিমেন্সের ইন্ডাস্ট্রিয়াল সফটওয়্যার। এ ধরনের সফটওয়্যার ব্যবহার করে হামলার চালানোর মূল লক্ষস্থল ইরান। স্টাক্সনেট ওয়ার্মের জন্মস্থান নিয়ে বেশ গুজবের জন্ম দেয় এর লক্ষস্থলের কারণে। এই কমপিউটার ওয়ার্ম বুশেহর নিউক্লিয়ার রিয়েক্টরের ল্যাপটপগুলোকে সংক্রমিত করে। এর ফলে ইরানের প্রথম নিউক্লিয়ার প্লান্টের চালু করা কার্যক্রমকে ব্যাহত করে অর্থাৎ পিছিয়ে দেয়। প্রথমেই এই ওয়ার্ম ম্যানেজ করে নেয় অদৃশ্য হয়ে থাকার উপায়। এই ওয়ার্ম শনাক্ত হওয়ার পর ব্যাপকভাবে গুজব ছড়িয়ে পড়ে যে এই ওয়ার্ম যুক্তরাষ্ট্র ও ইসরায়েলের নিরাপত্তা বাহিনীর তৈরি। শোনা যায়, ইরানের বিতর্কিত পারমাণবিক কর্মসূচির তথ্য জানার জন্য সাইবার গোয়েন্দা হিসেবে তারা এই ওয়ার্ম তৈরি করেছে। এটি অন্যান্য ওয়ার্ম থেকে বৈশিষ্ট্যসূচকভাবে আলাদা এবং রহস্যময়, কেননা এটি আক্রান্ত করে সিস্টেমে মারাত্মক কোনো ক্ষতি করে না। প্রথম দিকে মনে করা হতো, স্টাক্সনেট তৈরি করা হয় গোয়েন্দাগিরির জন্য। কিন্তু এটি তৈরি করা হয়েছে ধ্বংস করার জন্য। এতে স্পষ্ট বুঝা যাচ্ছে, স্টাক্সনেট ডেভেলপারদের টার্গেট সিস্টেমে ভর করে থাকা, কোনোভাবে আবিষ্কৃত না হয়ে সেখানেই অবস্থান করবে দীর্ঘ সময় ধরে এবং আড়াল থেকে প্রসেসকে পরিবর্তন করতে থাকবে তবে কোনো ক্ষতি না করে। এই ম্যালওয়্যার স্যাবোটাজ বা ধ্বংস করে না শুধু ফ্রিকোয়েন্সি কনভার্ট করে।

ইরানভিত্তিক কোম্পানি Fararo Paya বা ফিনল্যান্ড ভিত্তিক Vacon কোম্পানি দু'টি থেকে নির্দিষ্ট অ্যাপ্লিকেশনে ৮০৭ হার্টজ এবং ১২১০ হার্টজ গতির মধ্যে ফ্রিকোয়েন্সি চালিত হয়। সিমেনটেক অত্যন্ত সতর্কতার সাথে পর্যবেক্ষণ করে দেখে, স্টাক্সনেটের টার্গেট ছিল ইরানের নিউক্লিয়ার রিয়েক্টর, কিন্তু তারা তা প্রকাশ করেনি। স্টাক্সনেট আক্রান্ত হার্ডওয়্যারে তার পথ খুঁজে নেয় নেটওয়ার্কে ।

একই ধরনের ঘটনা ঘটে ২০০৮ সালে ইউএস সেন্ট্রাল কমান্ড (CENT COM)-এ। ইউএস সেন্ট্রাল কমান্ডে ইউএসবি ফ্ল্যাশ ড্রাইভের মাধ্যমে Agent.btz নামের এক ভাইরাস ছড়িয়ে পড়ে কমপিউটারে। এটি কোনো ক্ষতি করতে পারেনি বা বিশেষ ধরনের তথ্যকে অনাকাঙ্ক্ষিত অ্যাক্সেসের জন্য দুয়ার উন্মুক্ত করে দেয়নি। সাধারণত বিশেষ ধরনের ডাটাসম্বলিত ল্যাপটপের সাথে সূক্ষ্ম ইন্টারনেট সংযোগ থাকে। এই ভাইরাস কোনো ক্ষতি করতে না পারলেও রহস্যময় হিসেবে চিহ্নিত হয়ে আছে এবং এর উৎস এখনও জানা যায়নি।

সম্প্রতি ড্রোনেও ভাইরাস শনাক্ত হয়েছে, যা সম্ভবত রহস্যাবৃত থেকেই যাবে। বিশেষ সূত্রে জানা যায়, ভাইরাস এবং এর কিলগার হলো 'logging pilot' যা প্রতিটি কিস্ট্রোককে



আফগানিস্তান ও অন্যান্য ওয়ারজোনের মিশনে উড়ে যায়। কিন্তু Agent.btz আক্রান্ত 'ইউএস সেন্ট্রাল কমান্ড' কমপিউটারের ক্ষেত্রে ভাইরাস ইন্টারনেট থেকে আসেনি। Predator এবং Reaper ব্যবহার করে রিমুভেবাল হার্ডড্রাইভ যাতে ম্যাপ আপডেট লোড করে এবং মিশন এক মেশিন থেকে আরেক মেশিনে ভিডিও ট্রান্সপোর্ট করে। বিশেষজ্ঞেরা মনে করেন, এই ভাইরাস রিমুভেবাল হার্ডড্রাইভের মাধ্যমে বিস্তৃত হয়েছে। সুতরাং এখন প্রশ্ন হলো–এ ভাইরাস ক্লাসিফায়েড নেটওয়ার্কে বিদ্যমান থেকে নেটওয়ার্কের বাইরে কাউকে তথ্য পাঠাতে পারবে কী? এটি সন্দেহজনক হলেও এমন ব্যাপার ঘটেছে, কেননা ক্লাসিফায়েড নেটওয়ার্কে সূক্ষ্ম ইন্টারনেট সংযোগ থাকে। এক্ষেত্রে সংক্রমিত ফ্ল্যাশ ড্রাইভের ভাইরাস খুব সহজেই নেটওয়ার্কে এন্টার করতে পারে। তবে সেন্ডারের সাথে ভাইরাসের যোগাযোগ রক্ষা করার ব্যাপারটি কঠিন ও অবিশ্বাস্য। ফ্ল্যাশ ড্রাইভ তাই কমপিউটার নেটওয়ার্কে ম্যালওয়্যার নিয়ে আসতে পারে। এগুলোও সিকিউরিটি ঝুঁকিতে আছে। ফ্ল্যাশ ড্রাইভ গুরুত্বপূর্ণ ডাটা হারানোর কারণ হয়ে দাঁড়াতে পারে, যদি গুরুত্বপূর্ণ ডাটা ফ্ল্যাশ ড্রাইভে স্টোর করা হয়।

যুক্তরাষ্ট্রের জাতীয় পর্যায়ে আরেকটি উল্লেখযোগ্য সাইবার হামলা হলো, যুক্তরাষ্ট্রের ইনস্টিটিউশনের বিরুদ্ধে পরিচালিত সিরিয়াল সাইবার হামলা। এই হামলাগুলোকে মোটামুটিভাবে বর্ণনা করা হয় Titan Rain-এর অন্তর্গত নামে। ২০০৩ সালে যুক্তরাষ্ট্রের সমশ্রেণীভুক্ত কমপিউটার নেটওয়ার্কে বেশকিছু সাইবার হামলা হয়। এসব হামলায় হ্যাকারেরা হাতিয়ে নেয়ার চেষ্টা করে গুরুত্বপূর্ণ সব ফাইল, যেগুলো এরা পেয়েছে। হ্যাকারদের লক্ষ্য ছিল দেশের মিলিটারি সংশ্লিষ্ট সংবেদনশীল গুরুত্বপূর্ণ তথ্য, প্রতিরক্ষা ঠিকাদার এবং অ্যারোস্পেস সংশ্লিষ্ট। এ আইডেন্টি হ্যাকারদের এখন পর্যন্ত শনাক্ত করা যায়নি। তবে সবাই স্বীকার করেন, এই হামলাগুলো ছিল চমৎকার সমন্বয়মূলক। এক্ষেত্রে হ্যাকারেরা ব্যবহার করে বিশেষ এক টুল, যা ডিজাইন করা হয়েছে গোয়েন্দাগিরি কাজের জন্য। একে বলা হয় সাইবার স্পিয়নেজ।

এখানে উল্লিখিত সব সাইবার হামলার কমন বা সাধারণ বিষয় হলো–এগুলোর সবই আক্রান্ত মিডিয়াতে অদৃশ্যভাবে বিদ্যমান থাকে তাদের উদ্দেশ্য হাসিলের জন্য। ২০০৭ সালের এস্তোনিয়ার সাইবার হামলাটি ছিল একটু ভিন্ন। এই হামলাটি নীরব গোয়েন্দা হামলা ছিল না। এস্তোনিয়ায় হ্যাকারেরা সরকারের মন্ত্রণালয়, রাজনৈতিক দল, সংবাদপত্র, ব্যাংক এবং কোম্পানির ওয়েবসাইটগুলো ডিজ্যাবল করে ফেলে। এক্ষেত্রে ন্যাটো সক্রিয় হয়ে ওঠে এবং সিদ্ধান্ত নেয় Tallinn নামের একজন সাইবার টেরোরিজম বিশেষজ্ঞ পাঠানোর। একজন প্রো-ক্রেমলিন দেশপ্রেমিক যুবক এই সাইবার হামলার দায়ভার স্বীকার করে বলেন, এটি তার ব্যক্তিগত প্রতিবাদ।

কোনো কোনো সোর্সের ধারণা এই সাইবার হামলার জন্য দায়ী ছিল ২০০৫ ও ২০০৭ সালের Rio de Janeiro-এর অংশে ব্ল্যাকআউট। তবে এর কোনো সত্যতার প্রমাণ পাওয়া যায়নি। যদিও সাইবার হামলার জন্যই ব্ল্যাকআউট হয়েছিল বলে ধারণা করা হয়। তাদের মতে এটি দুর্ভাগ্যজনক এবং অনাকাঙ্ক্ষিত ঘটনা যে, এ ধরনের হামলার জন্য রাষ্ট্রের একজন অ্যাক্টর তথা কর্মকর্তা জড়িত। বাংলাদেশের সরকারি ওয়েবপোর্টালে এক হামলা হয় ২০১০ সালের ২০ মার্চ। দেশের ১৯ জেলার ওয়েবপোর্টালে ▸

এই সাইবার হামলা দেশে ব্যাপক আলোড়ন সৃষ্টি করে। অবশ্য এতে দেশের গুরুত্বপূর্ণ তথ্য হাতিয়ে নেয়ার মতো ঘটনা ঘটেনি।

সাইবার স্পেস থেকে নিরাপত্তার হুমকি

যদি সমগ্র বিশ্ব ইন্টারনেটের মাধ্যমে সংযুক্ত থাকে, তাহলে তো সাইবার হামলা শুধু একটি জাতীয় হুমকি হিসেবে গণ্য করা যায় না। কমপিউটার ভাইরাস, ওয়ার্ম ও বুটনেট ইত্যাদি বিশ্বজুড়ে কমপিউটারকে আক্রান্ত করতে পারে, বিশেষ করে যেগুলো ইন্টারনেটে যুক্ত। সুতরাং বিশ্বের সব দেশের সরকার ও কোম্পানিকে ইলেকট্রনিক ডাটা প্রসেসিং ব্যবহার করে তাদেরকে ডাটা নিরাপদ রাখার উপায় বের করতে হবে।

সাইবার সিকিউরিটি সম্পর্কে ভাবার আগে আপনাকে যথাযথভাবে নির্ধারণ করতে হবে কোনগুলোকে নিরাপদ রাখতে হবে। এই নিরাপদ রাখার পরিমাপ বা মাত্রাকে সাধারণ টার্মে অভিহিত করা হয় সাইবার সিকিউরিটি হিসেবে। কমপিউটার ও নেটওয়ার্কে অনাকাঙ্ক্ষিতভাবে অ্যাক্সেসকে সাইবার অ্যাটাক বা সাইবার হামলা বলা হয়। এখন প্রশ্ন হচ্ছে, সাইবার স্পেসের মাধ্যমে অনাকাঙ্ক্ষিত ব্যক্তিরা কিভাবে ইন্টারনাল নেটওয়ার্ক ও প্রসেসে অ্যাক্সেস পায়। এক্সটারনাল ও কমপিউটার নেটওয়ার্কে অ্যাক্সেসের সহজ ও সরলতম উপায় হলো সিকিউরিটি গ্যাপ বা ত্রুটিকে কাজে লাগানো। এই সিকিউরিটি গ্যাপ থাকতে পারে সরকারি ও বেসরকারি প্রতিষ্ঠানে ব্যবহার হওয়া সফটওয়্যার ও হার্ডওয়্যারের মধ্যে। তবে সবচেয়ে বড় সিকিউরিটি ঘাটতি বা ত্রুটি হলো সিস্টেম অ্যাডমিনিস্ট্রেশনে যা ব্যবহারকারীকে সিস্টেমে অ্যাক্সেস করার অনেক বেশি সুযোগ দেয়। যেহেতু ব্যবহারকারী সিস্টেমে অ্যাক্সেসের অনেক বেশি সুযোগ পায়, তাই ঝুঁকিও অনেক বেশি। যদি ম্যালওয়্যার ইমেইলে যুক্ত থাকে অথবা এক্সটারনাল স্টোরেজ ডিভাইস যেমন ইউএসবি ফ্ল্যাশ ড্রাইভে থাকে, তাহলে অবৈধ অনুপ্রবেশকারীরা সহজে সিস্টেমে অ্যাক্সেস করতে পারবে এবং চুরি করতে পারবে গুরুত্বপূর্ণ ডাটা অথবা ডাটা ম্যানুপুলেট করতে পারবে।

প্রাইভেট বা সাধারণ ব্যবহারকারীরা হুমকির মুখে

সাইবার অপরাধীদের প্রধান টার্গেট সাধারণ জনগণ। কেননা সাইবার অপরাধীদের টার্গেট অনলাইন ব্যাংকিং অ্যাকাউন্ট, ইমেইল অ্যাকাউন্টে অ্যাক্সেস করার মাধ্যমে অর্থ হাতিয়ে নেয়া বা ক্রেডিট কার্ড প্রতারণা করা। কখনো কখনো সাধারণ ব্যবহারকারীরা প্রতারণার বিষয়টি অনেক দেরিতে বুঝতে পারেন, আবার অনেকেই একেবারেই বুঝতে পারেন না। বাংলাদেশের সাধারণ ব্যবহারকারী ও কোম্পানির জন্য অন্যতম প্রধান হুমকি হলো স্ক্যাম। স্ক্যাম হচ্ছে ইমেইল মাধ্যমে প্রতারণা করা। সাধারণত স্ক্যাম পরিকল্পনাকারীরা তার সম্ভাব্য শিকারকে ইমেইলের মাধ্যমে প্রলোভন দেখায় যে, ব্যবহারকারী লটারিতে বিজয়ী হয়েছেন বা স্কলারশিপ পেয়েছেন বা গ্রিনকার্ড পেয়েছেন বলে ব্যবহারকারীকে ক্রেডিট কার্ড নম্বর বা ব্যাংক অ্যাকাউন্ট নাম্বার দিতে বলে। এসব তথ্য জেনে নিয়ে এরা প্রতারণা করে। প্রতারকেরা এভাবে স্ক্যামের মাধ্যমে কোটি কোটি ইউএস ডলার হাতিয়ে নিচ্ছে। বাংলাদেশেও স্ক্যামের মাধ্যমে প্রতারণা ব্যাপকভাবে বেড়ে গেছে এবং এটি এখন এক বড় সমস্যা হিসেবে চিহ্নিত হচ্ছে। এদের সম্ভাব্য শিকার বিশ্ববিদ্যালয়ের ছাত্র-ছাত্রী, যারা পড়াশোনার জন্য বিদেশে যেতে চায় বা স্কলারশিপের জন্য চেষ্টা করছে বা চাকরির জন্য গ্রিনকার্ড প্রত্যাশা করছে বা চাকরি প্রত্যাশীরা।

রহস্যময় সাইবার গোয়েন্দা

সাইবার গোয়েন্দারা কোনো কোম্পানির জন্য তেমন কোনো হুমকি নয়। সরকার ও এর কৌশলগত গুরুত্বপূর্ণ বিষয় সাইবার গোয়েন্দাদের টার্গেট। সাধারণত বেশিরভাগ দেশের সাইবার গোয়েন্দারা কাজ করে নিজ দেশের সরকারের পক্ষ অবলম্বন করে। তাই সাইবার গোয়েন্দারা অন্য দেশের সরকারের নেটওয়ার্কে অ্যাক্সেস করে গুরুত্বপূর্ণ ডাটা হাতিয়ে নেয়ার চেষ্টা করে যেসব বিষয় সাধারণত সরকার দেশের জনসাধারণের সামনে উপস্থাপন করে না।

নেটওয়ার্কে অ্যাক্সেসের সহজতম উপায় হলো ট্রোজান হর্সেস ব্যবহার করা, বিশেষ করে যদি নেটওয়ার্কে সিকিউরিটি সংশ্লিষ্ট ত্রুটি বা দুর্বলতা থাকে। যদি নেটওয়ার্কে সিকিউরিটি সংশ্লিষ্ট দুর্বলতা থাকে তাহলে ব্যবহারকারী উপদ্রবসহ ইমেইল ওপেন করা মাত্রই ট্রোজান হর্সেস সক্রিয়হয়ে উঠতে পারে। সাইবার গোয়েন্দারা বিকল্পভাবে ফিশিং মেইল সেন্ড করতে পারে যা দেখে মনে হতে পারে বিশ্বাসযোগ্য কোনো সেন্ডার পাঠিয়েছে। জুন ২০১১ -এ ওয়াল স্ট্রিট জার্নালে প্রকাশিত এক নিবন্ধ থেকে জানা যায়, এ ধরনের ঘটনা ঘটেছে যুক্তরাষ্ট্রের এক কেবিনেট সদস্যসের ক্ষেত্রে। তিনি যখন ট্রোজান হর্স সম্বলিত এক ইমেইল অ্যাটাচমেন্ট ওপেন করেন, এর ফলে সেই মাসে তার সব ইমেইল কমিউনিকেশনে অনাকাঙ্ক্ষিতভাবে অবৈধ ব্যক্তিরা অ্যাক্সেস পেয়ে যায়।

প্রায় সময় ধারণা করা হয়, চীন হলো সবচেয়ে বড় সাইবার গোয়েন্দা হামলাকারী দেশ। ১৯৯৮ সালে পেন্টাগনের কমপিউটার নেটওয়ার্ক কয়েক দিনের জন্য সাইবার গোয়েন্দা হামলায় আক্রান্তহয়েছিল। যুক্তরাষ্ট্রের সরকারের গুরুত্বপূর্ণ কর্মকর্তারা বলেন, চীন এ হামলার জন্য দায়ী। অবশ্য চীন তা অস্বীকার করে।

ডিজিটাল বাংলাদেশের সিকিউরিটি চ্যালেঞ্জ

ডিজিটাল বাংলাদেশের লক্ষ্য পূরণের জন্য ক্ষমতাসীন আওয়ামী লীগ সরকার বিশ্বাস করে বাংলাদেশকে সম্পূর্ণরূপে ডিজিটালাইজ করতে হলে দেশের সব বিশ্ববিদ্যালয়, স্কুল, কলেজ, মাদ্রাসা, হাসপাতালসহ সরকারি প্রতিষ্ঠানগুলোকে ২০২১ সালের মধ্যে ইন্টারনেটের সাথে যুক্ত করতে হবে। একই সাথে কোম্পানিগুলোকে অফার করতে হবে বেশি থেকে বেশি অনলাইন সার্ভিস, যাতে অনলাইন শপিং বা কেনাকাটা, অনলাইন ব্যাংকিং এবং ইমেইল কমিউনিকেশন আরো ব্যাপকতা পায় এবং এর ফলে আরো বেশি গুরুত্ব পাবে বাংলাদেশের ডিজিটালাইজ কার্যক্রম। তবে অনলাইন কার্যক্রম যত বাড়বে তার সাথে সাথে বাড়বে এদেশে ডিজিটাল অপরাধের মাত্রা। অপরাধীরা ডিজিটাল বিশ্বে তাদের পথ বের করে নেবে। ডিজিটালাইজ দেশে ফিশিং, হ্যাকিং, ব্যক্তিগত ডাটা চুরি হওয়ার ঘটনা নিত্যনৈমিত্তিক ব্যাপার। শুধু তাই নয়, সরকারি প্রতিষ্ঠান ও কোম্পানিগুলোও হুমকির মুখে পড়ছে, যা পুরো দেশের জনগণের দৈনন্দিন জীবনকে প্রভাবিত করে। এর ব্যতিক্রমবাংলাদেশেও দেখা যায় না।

আমাদের দেশে সাইবার সিকিউরিটি কিভাবে সম্ভব, যেখানে শতকরা ৯০ ভাগ সফটওয়্যারই পাইরেটেড। পাইরেটেড সফটওয়্যারের সাথেই আসে ট্রোজান-হর্স বা অন্যান্য ধরনের ম্যালওয়্যার। পাইরেটেড সফটওয়্যার ও উইন্ডোজের পাইরেটেড ভার্সনের থাকে প্রচুর লুপ হোল, যা হ্যাকারদের প্রধান অস্ত্র। অবশ্য লাইসেন্স করা সফটওয়্যার কিন্তু সাইবার সিকিউরিটির মূলে নেই। তবে নেটওয়ার্ককে নিরাপদ রাখার জন্য আপ-টু-ডেট সফটওয়্যার ও সফটওয়্যার প্রোটেকশন খুবই গুরুত্বপূর্ণ। সম্প্রতি পাইরেটেড উইন্ডোজ ভার্সন ব্যবহারে নিরুৎসাহিত করার জন্য মাইক্রোসফট রুল আউট করে উইন্ডোজ জেনুইন অ্যাডভান্টেজ (WGA) সিস্টেম, যা উইন্ডোজ প্লাটফরমে পাইরেসি রোধে লড়াই করে যাবে। ভয় হলো উইন্ডোজের পরবর্তী আপডেট আরো খারাপভাবে ব্যবহারকারীর অভিজ্ঞতাকে প্রভাবিত করতে পারে, যেমন চীন উইন্ডোজ অপারেটিং সিস্টেমকে অবৈধভাবে কপি করে ব্যবহারকারীকে দিচ্ছে। সেই অপারেটিং সিস্টেম ব্যবহার করে ব্যবহারকারী 'black screen'-এ মুখোমুখি হচ্ছে। তাই যদি কম বাজেটেও আপডেট সফটওয়্যার পাওয়া সম্ভব হয়, তাহলে তা ব্যবহার করা উচিত। এক্ষেত্রে লিনআক্স ব্যবহার করা যেতে পারে।

সম্প্রতি বাংলাদেশ দেয়েল নামের ল্যাপটপ উৎপাদন ও বাজারজাত করছে, তা মূলত লিনআক্স অপারেটিং সিস্টেম বা গুগল অ্যান্ড্রোয়িড চালিত। যদি অন্যান্য সফটওয়্যার ক্রয়ক্ষমতার বাইরে থাকে, তাহলে বিকল্প হিসেবে লিনআক্স ব্যবহার করা যেতে পারে। এটি ওপেন সোর্স সফটওয়্যার। অবশ্য এই সফটওয়্যার ব্যবহার করতে চাইলে নেটওয়ার্ক ও সিকিউরিটি সম্পর্কে গভীর জ্ঞান থাকা দরকার। কারণ, এক্ষেত্রে প্রথম গুরুত্বপূর্ণ ধাপ হলো সাইবার সিকিউরিটি সম্পর্কে ভালো জ্ঞান থাকা। তাই নেটওয়ার্ক ও সফটওয়্যার সম্পর্কে ভালো জ্ঞান থাকলে সাইবার হুমকি থেকে নেটওয়ার্ককে রক্ষা করা সম্ভব। অনুরূপভাবে স্কুল, কলেজ ও বিশ্ববিদ্যালয়ে কমপিউটার শিক্ষার সময় প্রাইভেট কোম্পানির নিয়মকানুন সম্পর্কেও শিক্ষা দেয়া খুবই দরকার। যাতে কমপিউটার ব্যবহারের শুরুতে বৈধ-অবৈধ সফটওয়্যার সম্পর্কে সবাই সচেতন হতে পারে।

বাংলাদেশের বেশিরভাগ প্রতিষ্ঠান এখনো অফলাইনভিত্তিক। বর্তমান সরকারের লক্ষ্য ২০২১ সালের মধ্যে ডিজিটাল বাংলাদেশ প্রতিষ্ঠা করা। প্রধানমন্ত্রী শেখ হাসিনা তার এ লক্ষ্য পূরণের জন্য ঘোষণা দেন– 'বাংলাদেশের প্রতিটি অংশ আনা হবে ই-গভর্ন্যান্সের আওতায়, ডিজিটাল ডিভাইড কমানোর জন্য টেলিকমিউনিকেশন সিস্টেমকে আধুনিকায়ন করা হচ্ছে।' একই সাথে দেশের সবাই যদি তাদের ব্যক্তিগত সব তথ্য কমপিউটারে জমা করে, তাহলে প্রাইভেসি একটি ইস্যু হতে পারে।

আর তা সাইবার অপরাধীদের মাধ্যমে আক্রান্ত হতে পারে। সরকারকে যেমন তার নাগরিকদের ডাটা রক্ষা করতে হবে, তেমনি সরকারকেও সাইবার গোয়েন্দা ও সন্ত্রাসীদের হাত থেকে তার নিজের ডাটা ও কমিউনিকেশনকে রক্ষা করতে হবে।

বাংলাদেশে ইলেকট্রনিক ভোটিং মেশিন ব্যবহারের ক্ষেত্রে সাইবার সিকিউরিটি আরেকটি প্রশ্ন জন্ম দিয়েছে। কেননা, বিশ্বের অন্যান্য দেশের ইলেকট্রনিক ভোটিং মেশিন ব্যবহারের অভিজ্ঞতায় দেখা গেছে যে, ইলেকট্রনিক ভোটিং মেশিন অনেক সমস্যা সৃষ্টি করতে পারে এবং নির্বাচনের ফলাফল দিতে পারে। জার্মানভিত্তিক হ্যাকার অ্যাসোসিয়েশন-ক্যাওয়াস কমপিউটার ক্লাব তথা সিসিসি ইলেকট্রনিক ভোটিং মেশিন নিষিদ্ধ করার দাবি জানিয়েছে। সিসিসি প্রকাশ করেছে এর পুঙ্খানুপুঙ্খ এক জরিপের ফলাফল। এই জরিপের তথ্যানুযায়ী জানা যায়, ইলেকট্রনিক ভোটিং মেশিনে গোপনীয়তা রক্ষার ব্যাপারে অনেক ত্রুটি রয়েছে এবং খুব সহজেই ম্যানিপুলেট হতে পারে।

বাংলাদেশের ব্যাংক খাতের সাইবার সিকিউরিটি আরেকটি মারাত্মক হুমকির মুখে রয়েছে, যা বাংলাদেশের অর্থনীতির মারাত্মক ক্ষতি করতে পারে। বাংলাদেশের অনলাইন ব্যাংকিং এবং ক্রেডিট কার্ডের ব্যবহার তেমন ব্যাপক হয়নি। তবে গ্লোবালাইজড বিশ্বে অনলাইন ফিন্যান্সিয়াল ট্রানজেকশন এবং ব্যাপকভাবে গ্রহণযোগ্য ক্রেডিট কার্ডের গুরুত্ব ও এর ব্যবহার দিন দিন বেড়েই যাচ্ছে বিভিন্ন কোম্পানিতে এবং তাদের গ্রাহকদের কাছে।

ইলেকট্রনিক পেমেন্ট মেথডের প্রসারের সাথে সাথে অনলাইন সিকিউরিটি ও ব্যাংক প্রশ্নের মুখোমুখি হচ্ছে ব্যাপকভাবে। বিশেষ করে যদি সাইবার অপরাধীরা ব্যাংক অ্যাকাউন্ট খালি করে ফেলে বা চুরি হওয়া ক্রেডিট কার্ডের তথ্যের অপব্যবহার হয়, তার জন্য দায়ী সাইবার অপরাধীরা।

বাংলাদেশের সাইবার সিকিউরিটির অবস্থা উন্নত করার গুরুত্বপূর্ণ ধাপ হলো ডিজিটালাইজড ডাটা ও নেটওয়ার্কে শ্রেণীবিন্যাস করা। তবে তা বাস্তবায়ন করা সবার সাধ্যের মধ্যে নয়, কেননা এজন্য সেটআপ করতে হয় এক টাস্কফোর্স, যার লক্ষ্য হবে সাইবার সিকিউরিটি বাস্তবায়ন ও সাইবার হামলাকে অ্যানালাইসিস করা। একই সাথে জনগণকে সাইবার হুমকি সম্পর্কে ব্যাপকভাবে সচেতন করতে হবে এবং প্রমাণ করতে হবে বাংলাদেশ সাইবার হামলা থেকে নিরাপদ।

লক্ষণীয়, ইন্টারনেট সংযোগ ও কমপিউটার শিক্ষা বেড়ে যাওয়ার সাথে সাথে সাইবার অপরাধী যেমন বাড়ছে, তেমনি সাইবার অপরাধীদের হামলার কৌশলও অনেক নিখুঁত ও ভয়াবহ হয়ে উঠছে। সুতরাং এই বিষয়টিকে গুরুত্বের সাথে বিবেচনা করে আমাদেরকে এগিয়ে যেতে হবে।

ক্যারিয়ার হিসেবে সাইবার সিকিউরিটি

যুক্তরাষ্ট্রসহ ইউরোপীয় ইউনিয়নের দেশগুলোর বিভিন্ন কোম্পানি যেকোনো ধরনের সাইবার হামলা প্রতিহত করার জন্য নিজ নিজ কোম্পানিতে ব্যাপকভাবে নিয়োগ দিচ্ছে সিকিউরিটি ইঞ্জিনিয়ার ও অ্যানালিস্টদের। যেহেতু প্রযুক্তি বিশ্বের মূল নিয়ন্ত্রক এখনো যুক্তরাষ্ট্র, তাই এ লেখা অবতারণা করা হয়েছে যুক্তরাষ্ট্রের প্রযুক্তির বাজারে আইসিটি পেশাজীবীদের সাম্প্রতিক চাহিদা ও নিয়োগদান প্রবণতার আলোকে। বিশেষজ্ঞরা মনে করেন, এ ধারা পরিলক্ষিত হচ্ছে বিশ্বের অন্যান্য দেশেও।

সাইবার সিকিউরিটি প্রফেশনালদের চাহিদা এমনভাবে বেড়ে গেছে যে যুক্তরাষ্ট্র সরকারকে খুব শিগগির এ সেক্টরের জন্য ন্যূনতম দশ হাজার বিশেষজ্ঞ ভাড়া করতে হবে এবং প্রাইভেট সেক্টরের জন্য ভাড়া করতে হবে চারগুণ বেশি। বিশেষজ্ঞদের মতে, সাইবার সিকিউরিটির ক্ষেত্রে এ সংখ্যা যুক্তরাষ্ট্রের জন্য খুবই নগণ্য, তাদের

দরকার আরো অনেক বেশি বিশেষজ্ঞ। যুক্তরাষ্ট্রের শিক্ষা ও ওয়ার্কফোর্সের ওপর জর্জটাউন ইউনিভার্সিটি সেন্টারের গবেষণাকর্মে দেখা যায়, শতকরা ছয় ভাগ কলেজ গ্র্যাজুয়েটের রয়েছে কমপিউটার এবং গণিতের ওপর ডিগ্রি। সেখানে সরাসরি সাইবার সিকিউরিটি সংশ্লিষ্ট বিষয়ে গ্র্যাজুয়েটের সংখ্যা শতকরা দুই ভাগ মাত্র।

বিশেষজ্ঞরা মনে করেন, হাই স্কুল শিক্ষা কার্যক্রমে প্রকৌশল, প্রযুক্তি এবং বিজ্ঞানের পাশাপাশি সাইবার সিকিউরিটি বিষয়ে প্রশিক্ষণের ব্যবস্থা রাখা দরকার। যুক্তরাষ্ট্রের ন্যাশনাল সায়েন্স ফাউন্ডেশন তথা এনএসএফ পরিকল্পনা করে ২০১৬-র মধ্যে ১০ হাজার কমপিউটার সায়েন্স ক্লাসের জন্য অর্থ সহায়তা দেবে।

হ্যাকার্স, সাইবার অপরাধী এবং বাইরের প্রতিদ্বন্দ্বী কোম্পানিগুলো গুরুত্বপূর্ণ তথ্য হাতিয়ে নেয়ার চেষ্টায় সবসময়ই লিপ্ত থাকে। তাই যুক্তরাষ্ট্রের বিভিন্ন প্রতিষ্ঠান সাইবার সিকিউরিটি বিশেষজ্ঞ ভাড়া করছে ব্যাপকভাবে এবং সংশ্লিষ্ট ক্ষেত্রে চাহিদা অতীতের যেকোনো সময়ের চেয়ে অনেক বেড়ে গেছে।

প্রায় সব ইন্ডাস্ট্রিতে সাইবার সিকিউরিটির বিশেষজ্ঞদের চাহিদা বেড়েই চলেছে। যেমন ফিন্যান্সিয়াল সার্ভিস, ম্যানুফ্যাকচারিং সেক্টর থেকে শুরু করে হেলথকেয়ার এবং রিটেইল মার্কেট পর্যন্ত সবক্ষেত্রেই। যুক্তরাষ্ট্রের প্রধান কোম্পানিগুলোতে সাইবার সিকিউরিটি সংশ্লিষ্ট পজিশনের জন্য লোক নিয়োগদান প্রবণতা ব্যাপকভাবে বেড়ে গেছে। ইউএস ফেডারেল গভর্নমেন্ট মার্কেটে সাইবার সিকিউরিটি বিশেষজ্ঞদের চাহিদা প্রচুর।

এদিকে আইটি সংশ্লিষ্ট পেশাজীবীদের জন্য ওয়েবসাইট Dice.com-এ তালিকাভুক্ত হয়েছে বেশ কিছু সাইবার সিকিউরিটি সংশ্লিষ্ট পেশা এবং এ সংখ্যা গত বছরের তুলনায় অনেক বেড়েছে। এই ওয়েবসাইটের তথ্যানুযায়ী দেখা যায়, আইসিটি সংশ্লিষ্ট পেশাগুলোর মধ্যে বর্তমানে সবচেয়ে বেশি চাহিদা হলো সাইবার সিকিউরিটি বিশেষজ্ঞদের। সম্প্রতি যুক্তরাষ্ট্রের কোম্পানিগুলো তাদের নিজেদের জন্য ভাড়া করছে হাজার হাজার নেটওয়ার্ক সিকিউরিটি, ইনফরমেশন সিকিউরিটি এবং অ্যাপ্লিকেশন সিকিউরিটি বিশেষজ্ঞ।

আইটি সংশ্লিষ্ট পেশাজীবীদের জন্য ওয়েবসাইট Dice.com-এ শীর্ষ পাঁচ চাহিদাসম্পন্ন সাইবার সিকিউরিটি সংশ্লিষ্ট পেশা হলো–

০১. সাইবার সিকিউরিটি অ্যানালিস্ট, ০২. সাইবার সিকিউরিটি ইঞ্জিনিয়ার, ০৩. সফটওয়্যার ইঞ্জিনিয়ার, ০৪. সিস্টেম ইঞ্জিনিয়ার ও ০৫. সিনিয়র সাইবার সিকিউরিটি অ্যানালিস্ট।

উত্তর আমেরিকার Dice.com সাইটের সিনিয়র ভাইস প্রেসিডেন্ট টম সিলভার বলেন, প্রতিবছরই সাইবার হুমকি বাড়ছে, আর তাই কোম্পানিগুলোকেও নিরাপত্তা বিধানের জন্য বিনিয়োগ বাড়াতে হচ্ছে। Dice.com সাইটের তথ্যানুযায়ী জানা যায়, সম্প্রতি ইনফরমেশন সিকিউরিটি পেশা সর্বকালের মধ্যে সর্বোচ্চ পর্যায়ে পৌঁছে গেছে। এই সাইটে আরো উল্লেখ করা হয়েছে যে সিকিউরিটি পেশাদারেরা প্রতিরোধ করবে নিরাপত্তার বেষ্টনী, নিরাপত্তা সংশ্লিষ্ট শূন্যস্থান পূরণের জন্য করণীয় কাজগুলো করবে এবং যথাযথ পরামর্শ দেবে কার্যকর পদক্ষেপ নেয়ার জন্য।

কিছু কিছু প্রবণতা চালিত করে সাইবার সিকিউরিটি বিশেষজ্ঞের চাহিদা। অনেক কোম্পানির নেটওয়ার্ক দিন দিন জটিল থেকে জটিলতর হয়ে পড়ছে, কেননা এসব কোম্পানিকে আগের যেকোনো সময়ের চেয়ে এখন অনেক বেশি ট্রানজেকশনকে প্রসেস করতে হয়, হ্যান্ডেল করতে হয় অনেক বেশি ডাটা। এসব কোম্পানি ব্যবহার করে ক্লাউড অ্যাপ্লিকেশন যেমন–সেলসফোর্স (Salesforce) এবং টেলেও (Taleo)। এর ফলে তাদের নেটওয়ার্কের বাইরে তথ্যের নিরাপত্তার জন্য তাদের প্রয়োজনকে সম্প্রসারণ করতে হয়। শুধু তাই নয়, তাদেরকে কাজ করতে হয় বিপুলসংখ্যক মোবাইল ডিভাইস ব্যবহারকারী যেমন স্মার্টফোন এবং ট্যাবলেট পিসি নিয়ে।

ফোর্স থ্রির (Force 3) কন্সালটিং সার্ভিসেস এবং প্রজেক্ট ম্যানেজমেন্টের ভাইস প্রেসিডেন্ট সু ▸

ভেরমা বলেন, সাইবার সিকিউরিটি দক্ষতার জন্য তিন বছর আগে যা দরকার ছিল, তা এখনকার দৃশ্যপট থেকে সম্পূর্ণ ভিন্ন। ক্রফটন এমডি একজন সরকারি কন্ট্রাক্টর, তার সিকিউরিটির টিমের জন্য ভাড়া করেন কয়েকজন সিনিয়র ইঞ্জিনিয়ার, সলিউশন আর্কিটেক্ট এবং অ্যানালিস্ট। ভেরমা আরো বলেন, তিন বছর আগে এক্ষেত্রে আইপ্যাড ছিল না। কিন্তু এখন আমাদেরকে ভাড়া করতে হচ্ছে সেসব বিশেষজ্ঞকে যারা আপনার ডিভাইস এবং কনজ্যুমারাইজেশন ট্রেন্ডকে বুঝতে পারবে। তিনি আরো বলেন, এখন সব কিছুই ক্লাউড ও মোবাইলে শিফট করছে। তাই আইটি সেন্টরের নিরাপত্তার জন্য এখন ফায়ারওয়াল ম্যানেজিংয়ের কথা তেমন গুরুত্ব পায় না। কেননা আইসিটি সেক্টরে নিরাপত্তার বিষয়টি ফায়ারওয়াল ম্যানেজ করাকেও ছাড়িয়ে গেছে। এখন এন্টারপ্রাইজ এনভায়রনমেন্টে তথ্যের নিরাপত্তার প্রশ্নে আরো সম্পৃক্ত হয়েছে ক্লাউড অ্যাপ্লিকেশন এবং ট্যাবলেট।

আইটি স্ট্যাফিং এজেন্সি ইয়োহর (YoH) সিনিয়র ভাইস প্রেসিডেন্ট ডন হ্যানসন বলেন, সাইবার সিকিউরিটি Ffgdb ভঙ্গের কারণে এককভাবে যুক্তরাষ্ট্রের মেধাস্বত্ব সম্পদ চুরি হয় বছরে ৪০০ বিলিয়ন ডলারের বেশি। তিনি পর্যবেক্ষণ করে দেখেন, সেসব ডেভেলপারের চাহিদা রয়েছে যারা সিকিউরিটি অ্যাপ্লিকেশন তৈরি করতে পারেন, সিকিউরিটি সার্টিফিকেশনসহ নেটওয়ার্ক ইঞ্জিনিয়ার এবং নিরাপদ সিস্টেম ও প্রসেস কিভাবে করতে হয় তা বোঝাতে সক্ষম এমন আর্কিটেক্ট। তিনি আরো বলেন, সেসব আইটি পেশাজীবীর দরকার আছে যারা সিকিউরিটি মনিটরিংয়ের কাজে লিপ্ত থাকেন, তথ্যের নিশ্চয়তা দেন এবং রেগুলেটরি কমপ্লায়েন্স। তিনি আরো বলেন, সবচেয়ে বেশি দরকার হলো কাটিং এজ টেকনোলজি নিয়ে কাজ করা। হ্যানসন বলেন, বর্তমানে অনেক ধরনের মোবাইল ডিভাইস রয়েছে। সুতরাং গুরুত্বপূর্ণ বিষয় হলো মোবাইল ডিভাইস ম্যানেজমেন্টের জন্য একটি লেয়ার যুক্ত করা এবং এই বাড়তি লেয়ার কিভাবে কাজ করে তা বোঝা।

হ্যানসন আরো বলেন, বিভিন্ন কোম্পানি সে ধরনের আইটি পেশাজীবীদের অনুসন্ধান করছে, যারা সিকিউরিটি ইনফরমেশন ইভেন্ট ম্যানেজমেন্ট, অবৈধ অনুপ্রবেশকারীদের শনাক্ত এবং ডাটা হারানো প্রতিরোধ করার পাশাপাশি নীতিগতভাবে হ্যাকিং সংশ্লিষ্ট সার্টিফিকেশনসহ ডিজিটাল ফরেনসিকে দক্ষ।

শেষ কথা

প্রতিদিন নিত্য-নতুন ডিজিটাল পণ্য আমাদের জীবনের অংশ হয়ে উঠেছে এবং সাইবার স্পেস থেকে আক্রান্ত হওয়ার জন্য আমাদেরকে ভালনারেবল করে ফেলছে। বর্তমানে জাতীয় নিরাপত্তার জন্য সাইবার হামলা তেমন হুমকি নয়। কেননা বেশিরভাগ ক্ষেত্রে সাইবার হামলার কারণে আর্থিক ক্ষতি হয় বা ব্যক্তিগত ডাটা হারিয়ে যায় বা ক্ষতিগ্রস্ত হয়। যতদূর মনে হয় রাষ্ট্রীয় অকাঠামোয় এমন কোনো সাইবার হামলা হয়নি, যা অন্য কোনো দেশ বা সন্ত্রাসী সংগঠন সম্পাদন করে যার জন্য আমাদের জাতীয় নিরাপত্তা হুমকির মুখে পড়বে।

সাইবার সিকিউরিটি বলতে বুঝায় ডাটা রক্ষা করার সক্ষমতাকে, যেগুলো রক্ষা করা দরকার। যদি ব্যবহারকারী, কোম্পানি এবং সরকার ব্যক্তিগত ও গুপ্ত ডাটা নির্দিষ্ট করতে এবং একই সাথে বিভিন্ন নিরাপত্তা উদ্যোগ নিতে ব্যর্থ হয়, তাহলে খুব সহজেই ডাটায় অবৈধ অ্যাক্সেস হবে বলা যায়। আগেই বলা হয়েছে, প্রাইভেট ইউজারেরা সাইবার অপরাধীদের হামলার হুমকির মুখে আছে। সুতরাং সাইবার হামলার বা ব্যক্তিগত ডাটা হারানো সম্পর্কে দেশের জনগণকে অবহিতকরণ ও সচেতন করার দায়িত্ব সরকারের। একই সময় দেশের মধ্যে সাইবার হুমকির মাত্রা নির্দিষ্ট করতে হবে সরকারকে। সাইবার ঝুঁকির মুখোমুখি হওয়ার জন্য বেছে নিতে হবে যথাযথ পদক্ষেপ।

সাইবার অপরাধ প্রতিরোধে সহায়তার জন্য সরকারি উদ্যোগে বাংলাদেশ টেলিযোগাযোগ নিয়ন্ত্রণ কমিশনের অধীনে বাংলাদেশ কমপিউটার সিকিউরিটি ইনসিডেন্ট রেসপন্স টিম তথা বিডি-সিএসআইআরটি গঠন করা হয়েছে। এর ওয়েবসাইটও চালু করা হয়েছে। যেকোনো ধরনের সাইবার অপরাধের শিকার হলে পরবর্তী পর্যায়ে সমস্যা অনুযায়ী পরামর্শ দেয়। এই ওয়েবসাইটের মাধ্যমে সাইবার অপরাধের বিরুদ্ধে জনগণকে সচেতন ও যথাযথ পরামর্শ দেয়া হয়। তাছাড়া আক্রান্তদের নিরাপত্তা ও গোপনীয়তা রক্ষা করতে সহায়তা করে। অনাকাঙ্ক্ষিত সমস্যা যেনো না ঘটে তার জন্য পরামর্শ দিয়ে সচেতন করা হয়। ওয়েবসাইট www.esirt.gov.bd.

ফিডব্যাক : mahmood@comjagat.com