সাইবার নিরাপত্তা: ভারতে সাইবার আইন

সাইবার নিরাপত্তা হ'ল নেটওয়ার্ক, কম্পিউটার, ডেটা এবং প্রোগ্রামগুলিকে অননুমোদিত আক্রমণ থেকে রক্ষা করার অনুশীলন। ইন্টারনেট, ওয়্যারলেস নেটওয়ার্ক এবং কম্পিউটার সিস্টেমের উপর নির্ভরতা বৃদ্ধির কারণে ভারতে সাইবার নিরাপত্তা অত্যন্ত গুরুত্বপূর্ণ হয়ে উঠছে। এছাড়াও স্মার্টফোন, টেলিভিশন এবং "ইন্টারনেট অফ থিংস" গঠনকারী বিভিন্ন ডিভাইসের ব্যবহার দ্রুত বৃদ্ধি সাইবার সিকিউরিটির প্রয়োজনীয়তা তৈরি করেছে। সাম্প্রতিক সময়ে, ভারতে সাইবার আইনও সারা বিশ্বের মানুষের জন্য একটি বড় ভীতি হয়ে উঠেছে।

সাইবার সিকিউরিটি WBCS Syllabus - র একটি অংশ, এবং যে সমস্ত প্রার্থী সিভিল সার্ভেন্ট হতে চান তাদের অবশ্যই এই বিষয়ে তথ্য জানতে হবে। এখানে আমরা ভারতের সর্বশেষ সাইবার আইনগুলির পাশাপাশি সাইবার সুরক্ষার সমস্ত বেসিকগুলি কভার করব।

সাইবার নিরাপত্তা কি?

সাইবার নিরাপত্তা সার্ভার, কম্পিউটার, ইলেকট্রনিক সিস্টেম, মোবাইল ডিভাইস, নেটওয়ার্ক এবং ডেটাকে দূষিত আক্রমণ থেকে রক্ষা করার একটি পদ্ধতি।

- সাইবার সিকিউরিটি কে বলা হয় Information Technology Security বা Electronic Information Security। সাইবার সিকিউরিটিতে ব্যবসা থেকে শুরু করে মোবাইল কম্পিউটিং পর্যন্ত একাধিক ডোমেইন রয়েছে।

- 'সাইবার' শব্দটি কম্পিউটার এবং কম্পিউটার নেটওয়ার্কের সাথে সম্পর্কিত। ইন্টারনেট ইকোসিস্টেমের মধ্যে সংযোগ সাইবারস্পেস গঠন করে এবং এই সাইবারস্পেস বিভিন্ন সমস্যার মধ্যে পড়লে সাইবার সুরক্ষার প্রয়োজনীয়তা পড়ে।

সাইবার নিরাপত্তার প্রয়োজনীয়তা

ভারতে সাইবার নিরাপত্তার গুরুত্ব ও প্রয়োজনীয়তা বোঝার জন্য; সাইবার নিরাপত্তার মৌলিক বিষয়গুলি ভালোভাবে বোঝা গুরুত্বপূর্ণ।

- একজন ব্যক্তির জন্য- ফটো, ভিডিও, বা সোশ্যাল নেটওয়ার্কগুলিতে কোনও ব্যক্তির দ্বারা শেয়ার করা ব্যক্তিগত তথ্য অন্যের দ্বারা অনুপযুক্তভাবে ব্যবহার হতে পারে, যা গুরুতর ঘটনা তৈরি করে।
- সরকারের জন্য- সরকারের কাছে দেশ এবং তার নাগরিকদের সম্পর্কে প্রচুর গোপনীয় তথ্য রয়েছে। যদি তথ্য ফাঁস হয়ে যায়, তাহলে তা দেশের জন্য মারাত্মক হুমকির জন্ম দেবে।
- ব্যবসার জন্য- ডেটা একটি ব্যবসার মেরুদণ্ড, এবং কোম্পানিগুলি তাদের সিস্টেমে প্রচুর পরিমাণে ডেটা এবং তথ্য সংরক্ষণ করে। সাইবার আক্রমণের ফলে গুরুত্বপূর্ণ তথ্যের ক্ষতি হতে পারে, গ্রাহকের ব্যক্তিগত ডেটার ক্ষতি হিসাবে সিঙ্ক হতে পারে, ইত্যাদি যদি ঘটে তবে সংস্থাটি জনসাধারণের বিশ্বাস হারাবে এবং সংস্থার সততা সম্পর্কে প্রশ্ন উঠতে পারে।

সাইবার নিরাপত্তার মূল বিষয়সমূহ

সাইবার আক্রমণের ঘটনা উল্লেখযোগ্যভাবে বৃদ্ধি পেয়েছে এবং এর সাথে সাথে, সাইবার নিরাপত্তা উদ্যোগগুলিও বিকশিত হয়েছে। প্রত্যেককে অবশ্যই ভারতে সাইবার সিকিউরিটির বেসিকগুলি জানতে হবে যাতে তারা নিজেদের রক্ষা করতে পারে।

- 1990-এর দশকে ভাইরাস মোকাবেলার জন্য অ্যান্টি-ভাইরাস এবং ফায়ারওয়ালের মতো কিছু সাইবার নিরাপত্তা উদ্যোগ তৈরি করা হয়েছিল।
- 2020 সালে ওর্মস মোকাবেলা করার জন্য, অনুপ্রবেশ সনাক্তকরণ এবং প্রতিরোধের উদ্যোগগুলি সংঘটিত হয়েছিল
- Botnets (2000s - বর্তমান) সমস্যা সমাধান করার জন্য, DLP, অ্যাপ্লিকেশন-সচেতন ফায়ারওয়াল, এবং SIM উন্নত করা হয়েছিল
- APT ইনসাইডার (বর্তমান) এর জন্য, নেটওয়ার্ক ফ্লো অ্যানালাইসিস উদ্যোগ নেওয়া হয়

সাইবার নিরাপত্তা এবং এর উপাদানসমূহ

একনজরে দেখে নেওয়া যাক সাইবার সিকিউরিটির উপাদানগুলো

- অ্যাপ্লিকেশন নিরাপত্তা- এটি সাইবার হুমকি থেকে রক্ষা করার জন্য একটি অ্যাপ্লিকেশনের বিকাশের সময় গৃহীত ব্যবস্থা।
- নেটওয়ার্ক নিরাপত্তা - এটি নেটওয়ার্কের নির্ভরযোগ্যতা, ব্যবহারযোগ্যতা, নিরাপত্তা এবং অখণ্ডতা রক্ষা করার জন্য নিরাপত্তা ব্যবস্থা অন্তর্ভুক্ত করে।

- তথ্য নিরাপত্তা - এটি গোপনীয়তা রক্ষা এবং চুরি এড়ানোর জন্য অননুমোদিত অ্যাক্সেস থেকে তথ্য সুরক্ষা।
- দুর্যোগ পুনরুদ্ধারের পরিকল্পনা- এই প্রক্রিয়াটির মধ্যে রয়েছে ঝুঁকি মূল্যায়ন করা, আক্রমণের জন্য পুনরুদ্ধারের পরিকল্পনা বিকাশ করা এবং অগ্রাধিকার প্রতিষ্ঠা করা।

ভারতে সাইবার আইন

এই ধরনের অপরাধ রক্ষা ও প্রতিরোধের জন্য ভারতে বিভিন্ন সাইবার আইন রয়েছে।

তথ্য প্রযুক্তি আইন, 2000

- 2020 সালের অক্টোবরে এটি অস্তিত্বলাভ করে এবং এটি ভারতীয় সাইবার আইন নামেও পরিচিত। এটি সমস্ত ই-লেনদেনকে আইনি স্বীকৃতি প্রদান করে।
- তথ্য প্রযুক্তি আইন 2000 -এ কম্পিউটার সিস্টেম, কম্পিউটার নেটওয়ার্ক, তথ্য এবং বৈদ্যুতিন বিন্যাসে তথ্যের ব্যবহার নিয়ন্ত্রণ করা হয়েছে।
- এই আইনটি নিম্নলিখিতগুলিকে অপরাধ হিসাবে তালিকাভুক্ত করে - একটি কম্পিউটার সিস্টেমের হ্যাকিং, কম্পিউটার নথিগুলিতে সাথে হস্তক্ষেপ করা, কম্পিউটার সম্পদ ব্যবহার করে প্রতারণা করা এবং সাইবার সন্ত্রাসবাদের কাজ।

জাতীয় সাইবার নীতি 2013

জাতীয় সাইবার নীতি 2013 এর অধীনে কৌশলগুলি নিম্নরূপ।

- নিরাপত্তা হুমকি এবং জাতীয় প্রক্রিয়া এবং সিস্টেমের মাধ্যমে প্রতিক্রিয়াগুলির জন্য একটি নিরাপদ সাইবার ইকোসিস্টেম এবং প্রক্রিয়া তৈরি করা।
- Public Key Infrastructure এবং global best practices এর ব্যবহার বাস্তবায়নের মাধ্যমে ই-গভর্নেন্স সুরক্ষিত করা।
- NCIIPC (National Critical Information Infrastructure Protection Centre) এর সাথে গুরুত্বপূর্ণ তথ্য অবকাঠামো সুরক্ষা
- প্রশিক্ষণ ও শিক্ষা কর্মসূচির মাধ্যমে মানব সম্পদ উন্নয়ন
- সাইবার নিরাপত্তা প্রযুক্তির উন্নয়ন।

জাতীয় সাইবার নিরাপত্তা কৌশল 2020

- ভারত সরকার ভারতে সাইবার স্পেস সুরক্ষিত করার জন্য জাতীয় সাইবার নিরাপত্তা কৌশল 2020 বাস্তবায়নের পরিকল্পনা করেছে।

সাইবার নিরাপদ ভারত উদ্যোগ

- MeitY ন্যাশনাল ই-গভর্নেন্স ডিভিশন (NeGD) এর সাথে সহযোগিতা করে এবং 2008 সালে একটি সাইবার-স্থিতিস্থাপক আইটি সেটআপ প্রতিষ্ঠার জন্য এই উদ্যোগটি নিয়ে আসে।

সাইবার নিরাপত্তা চ্যালেঞ্জ

ভারতে সাইবার নিরাপত্তা অনেক চ্যালেঞ্জের মুখোমুখি হয় যা নিম্নরূপ

- মানুষের মোবাইল ও ইন্টারনেটের ব্যবহার বেড়েছে
- কিছু ডিভাইসে কঠিন নিরাপত্তা অবকাঠামোর অভাব
- ভারতে সাইবার নিরাপত্তা নিয়ে সচেতনতার অভাব
- সন্ত্রাসীদের সাইবার স্পেসের ব্যবহার বাড়ছে
- সাইবার স্পেসে দুর্বলতা
- অনেক ক্ষেত্রে, আক্রমণ প্রযুক্তি প্রতিরক্ষা প্রযুক্তিকে পরাভূত করে

ভারতে সাইবার নিরাপত্তা

ভারতে সাইবার নিরাপত্তার জন্য সরকার কর্তৃক গৃহীত সাম্প্রতিক কয়েকটি উদ্যোগ এখানে দেওয়া হল।

ভারতে সাইবার নিরাপত্তার জন্য সরকারের উদ্যোগ	উদ্দেশ্যসমূহ

সাইবার নিরাপদ ভারত উদ্যোগ	সাইবার অপরাধ সম্পর্কে সচেতনতা ছড়িয়ে দিতে এবং CISO (চিফ ইনফরমেশন সিকিউরিটি অফিসার) এবং সরকারী বিভাগজুড়ে ফ্রন্টলাইন আইটি কর্মীদের জন্য সুরক্ষা ব্যবস্থা গ্রহণের ক্ষমতা গড়ে তুলতে 2018 সালে চালু করা হয়েছিল।
ন্যাশনাল সাইবার সিকিউরিটি কো-অর্ডিনেশন সেন্টার (NCCC)	রিয়েল-টাইম সাইবার হুমকি রোধ করার জন্য দেশে আসা ইন্টারনেট ট্র্যাফিক এবং যোগাযোগের মেটাডেটা স্ক্যান করার জন্য 2019 সালে চালু করা হয়েছিল।
সাইবার স্বচ্ছতা কেন্দ্র	এই প্ল্যাটফর্মটি 2017 সালে ইন্টারনেট ব্যবহারকারীদের ম্যালওয়্যার এবং ভাইরাসগুলি মুছে ফেলার জন্য তাদের ডিভাইস এবং কম্পিউটার ক্লিন রাখার জন্য চালু করা হয়েছিল

তথ্য নিরাপত্তা শিক্ষা ও সচেতনতা প্রকল্প (ISEA)	এই প্রকল্পের আওতায় 52টি প্রতিষ্ঠানের মাধ্যমে 1.14 লক্ষ মানুষকে প্রশিক্ষণ দেওয়া, যাতে সাইবার নিরাপত্তা ক্ষেত্রে সচেতনতা বৃদ্ধি এবং শিক্ষা, গবেষণা ও প্রশিক্ষণ প্রদান করা যায়।
আন্তর্জাতিক সহযোগিতা	সাইবার ইকোসিস্টেমকে শক্তিশালী করতে জাপান, মার্কিন যুক্তরাষ্ট্র, সিঙ্গাপুরের মতো বেশ কয়েকটি দেশের সঙ্গে যুক্ত হয়েছে ভারত। এটি ভারতকে সাইবার হুমকি মোকাবেলায় আরও ভাল হতে সহায়তা করবে।

সাইবার নিরাপত্তা ও সাইবার হামলা

নিম্নলিখিত সাইবার আক্রমণের ধরণগুলি যা বছরের পর বছর ধরে বিকশিত হয়েছে

- ম্যালওয়্যার- যে কোনও ধরণের সফ্টওয়্যারকে বোঝায় যা কেবলমাত্র একটি কম্পিউটার নেটওয়ার্ক, কম্পিউটার বা সার্ভারের ক্ষতি করার জন্য ডিজাইন করা হয়। ওর্মস, ভাইরাস, স্পাইওয়্যার এবং ট্রোজানগুলি বিভিন্ন ধরণের ম্যালওয়্যার।
- ফিশিং হল প্রতারণামূলক ই-মেইল এবং ওয়েবসাইট ব্যবহার করে ব্যক্তিগত তথ্য সংগ্রহের পদ্ধতি।

- DOS, DDOS- আক্রমণকারীরা হোস্ট নেটওয়ার্কের পরিষেবাগুলি ব্যাহত করে নেটওয়ার্ক বা মেশিনটিকে অনুপলব্ধ করে তোলে।
- SQL Injection- অনেক সার্ভিসার যা সেবা ও ওয়েবসাইটের ডাটা সংরক্ষণ করে SQL ব্যবহার করে তাদের ডাটাবেস পরিচালনা করতে। SQL ইনজেকশন আক্রমণ গোপনীয় তথ্য পেতে দূষিত কোড ব্যবহার করে এই ধরনের সার্ভারগুলিকে লক্ষ্য করে।
- সাইবার গুপ্তচরবৃত্তি- যখন কোনো গুরুত্বপূর্ণ প্রতিষ্ঠান বা সরকারের গোপনীয়তা ঝুঁকির মধ্যে থাকে, তখন গোপনীয় তথ্য হাতিয়ে নিতে কম্পিউটার নেটওয়ার্কের অবৈধ ব্যবহারের কারণে।
- সাইবার ওয়ারফেয়ার- কম্পিউটার প্রযুক্তি ব্যবহার করে তথ্য ব্যবস্থাকে আক্রমণ করে, বিশেষ করে সামরিক উদ্দেশ্যে।
- সোশ্যাল ইঞ্জিনিয়ারিং- এটি মানুষের মিথস্ক্রিয়ার উপর নির্ভর করে ব্যবহারকারীদের সুরক্ষিত গুরুত্বপূর্ণ তথ্য অর্জনের জন্য সুরক্ষা পদ্ধতিগুলি ভঙ্গ করার জন্য প্রতারিত করে।

সাইবার নিরাপত্তার জন্য আন্তর্জাতিক পদ্ধতি

ইন্টারন্যাশনাল টেলিকমিউনিকেশন ইউনিয়ন (ITU) জাতিসংঘের মধ্যে একটি বিশেষায়িত সংস্থা যা সাইবার নিরাপত্তা এবং টেলিযোগাযোগের বিষয়গুলির উন্নয়ন ও মানদন্ডীকরণে গুরুত্বপূর্ণ ভূমিকা পালন করে।

- বুদাপেস্ট কনভেনশন অন সাইবার ক্রাইম একটি আন্তর্জাতিক সংস্থা যা জাতীয় আইনগুলির মধ্যে সমন্বয় সাধন করে, দেশগুলির মধ্যে সহযোগিতা বৃদ্ধি করে এবং তদন্তের জন্য কৌশলগুলি উন্নত করে সাইবার অপরাধকে সম্বোধন করে।
- Internet Corporation for Assigned Names and Numbers (ICANN): একটি অলাভজনক সংস্থা যা সংখ্যাসূচক স্পেস এবং নেমস্পেস সম্পর্কিত বেশ কয়েকটি ডাটাবেসের রক্ষণাবেক্ষণ এবং পদ্ধতির সমন্বয় সাধন এবং নিরাপদ অপারেশনের জন্য নেটওয়ার্কের স্থিতিশীলতা নিশ্চিত করার জন্য দায়ী।
- ইন্টারনেট গভর্নেন্স ফোরাম (IGF)- IGF ইন্টারনেট গভর্নেন্স বিতর্কে বেসরকারী খাত, সরকার, এবং সুশীল সমাজের মতো সমস্ত স্টেকহোল্ডারদের একত্রিত করে।