സൈബർ സുരക്ഷ

സെർവറുകൾ, കമ്പ്യൂട്ടറുകൾ, ഇലക്ട്രോണിക് സിസ്റ്റങ്ങൾ, മൊബൈൽ ഉപകരണങ്ങൾ, നെറ്റ്‌വർക്കുകൾ, ഡാറ്റ എന്നിവയെ ക്ഷുദ്രകരമായ ആക്രമണങ്ങളിൽ നിന്ന് സംരക്ഷിക്കുന്നതിനുള്ള ഒരു രീതിയാണ് സൈബർ സുരക്ഷ.

- സൈബർ സുരക്ഷയെ ഇൻഫർമേഷൻ ടെക്നോളജി സെക്യൂരിറ്റി അല്ലെങ്കിൽ ഇലക്ട്രോണിക് ഇൻഫർമേഷൻ സെക്യൂരിറ്റി എന്നും അറിയപ്പെടുന്നു. സൈബർ സുരക്ഷയിൽ ബിസിനസ്സ് മുതൽ മൊബൈൽ കമ്പ്യൂട്ടിംഗ് വരെ ഒന്നിലധികം ഡൊമെയ്‌നുകൾ ഉൾപ്പെടുന്നു.
- 'സൈബർ' എന്ന പദം കമ്പ്യൂട്ടർ, കമ്പ്യൂട്ടർ നെറ്റ്‌വർക്കുകളുമായി ബന്ധപ്പെട്ടിരിക്കുന്നു. ഇന്റർനെറ്റ് ആവാസവ്യവസ്ഥകൾ തമ്മിലുള്ള ഈ ബന്ധം സൈബർസ്‌പേസ് രൂപപ്പെടുത്തുന്നു, കൂടാതെ ഈ സൈബർസ്‌പേസ് സൈബർ സെക്യൂരിറ്റിയുടെ ആവശ്യകതയിലേക്ക് നയിക്കുന്ന വിവിധ പ്രശ്നങ്ങൾ ഉൾക്കൊള്ളുന്നു.

സൈബർ സുരക്ഷ ആവശ്യകത

ഇന്ത്യയിലെ സൈബർ സുരക്ഷയുടെ പ്രാധാന്യവും ആവശ്യകതയും മനസ്സിലാക്കാൻ; സൈബർ സുരക്ഷയുടെ അടിസ്ഥാനകാര്യങ്ങൾ സമഗ്രമായി മനസ്സിലാക്കേണ്ടത് പ്രധാനമാണ്.

- വ്യക്തികൾക്ക്- സോഷ്യൽ നെറ്റ്‌വർക്കുകളിൽ ഒരു വ്യക്തി പങ്കിടുന്ന ഫോട്ടോകളോ വീഡിയോകളോ വ്യക്തിഗത വിവരങ്ങളോ മറ്റുള്ളവർക്ക് അനുചിതമായി ഉപയോഗിക്കാം, ഇത് ഗുരുതരമായ സംഭവങ്ങളിലേക്ക് നയിക്കും.
- സർക്കാർ- രാജ്യത്തെയും പൗരന്മാരെയും കുറിച്ച് ഗവൺമെന്റിന് ധാരാളം രഹസ്യാത്മക വിവരങ്ങൾ ഉണ്ട്. വിവരങ്ങൾ ചോർന്നാൽ അത് രാജ്യത്തിന് ഗുരുതരമായ ഭീഷണി ഉയർത്തും.
- ബിസിനസ്സിനായി- ഡാറ്റ ഒരു ബിസിനസ്സിന്റെ നട്ടെല്ലാണ്, കമ്പനികൾക്ക് അവരുടെ സിസ്റ്റത്തിൽ വലിയ അളവിലുള്ള ഡാറ്റയും വിവരങ്ങളും സംഭരിച്ചിരിക്കുന്നു. സൈബർ ആക്രമണങ്ങൾ ഉപഭോക്താക്കളുടെ സ്വകാര്യ ഡാറ്റ നഷ്ടപ്പെടുന്നത് പോലുള്ള നിർണായക വിവരങ്ങൾ നഷ്ടപ്പെടാനിടയുണ്ട്. അങ്ങനെ സംഭവിച്ചാൽ കമ്പനിക്ക് പൊതുവിശ്വാസം നഷ്ടപ്പെടും, കൂടാതെ ഇത് സ്ഥാപനത്തിന്റെ വിശ്വാസിതയെ ചോദ്യം ചെയ്യും.

സൈബർ സുരക്ഷയുടെ അടിസ്ഥാനങ്ങൾ

സൈബർ ആക്രമണ കേസുകൾ ഗണ്യമായി വർദ്ധിച്ചു, അതോടൊപ്പം സൈബർ സുരക്ഷാ സംരംഭങ്ങളും വികസിച്ചു. ഇന്ത്യയിലെ സൈബർ സുരക്ഷയുടെ അടിസ്ഥാനകാര്യങ്ങൾ എല്ലാവരും അറിഞ്ഞിരിക്കണം, അതിലൂടെ അവർക്ക് സ്വയം പരിരക്ഷിക്കാൻ കഴിയും.

- 1990-കളിൽ വൈറസിനെ നേരിടാൻ, ആന്റി വൈറസ്, ഫയർവാളുകൾ തുടങ്ങിയ ചില സൈബർ സുരക്ഷാ സംരംഭങ്ങൾ വികസിപ്പിച്ചെടുത്തു.
- 2020-ൽ വൈറസിനെ നേരിടലും, നുഴഞ്ഞുകയറ്റം കണ്ടെത്തലും പ്രതിരോധ നടപടികളും വികസിപ്പിച്ചെടുത്തു.
- ബോട്ട്നെറ്റുകളുടെ പ്രശ്നങ്ങൾ പരിഹരിക്കാൻ, DLP, ആപ്ലിക്കേഷൻ-അവയർ ഫയർവാളുകൾ, സിം എന്നിവ വികസിപ്പിച്ചെടുത്തു

സൈബർ സുരക്ഷയും അതിന്റെ ഘടകങ്ങളും

സൈബർ സുരക്ഷയുടെ ഘടകങ്ങൾ നോക്കാം

- ആപ്ലിക്കേഷൻ സെക്യൂരിറ്റി- സൈബർ ഭീഷണികളിൽ നിന്ന് ആപ്ലിക്കേഷനെ സംരക്ഷിക്കാൻ ഒരു വികസിപ്പിക്കുന്ന ഒരു രീതിയാണിത്.
- നെറ്റ്‌വർക്ക് സുരക്ഷ- നെറ്റ്‌വർക്കിന്റെ വിശ്വാസ്യത, ഉപയോഗക്ഷമത, സുരക്ഷ, സമഗ്രത എന്നിവ സംരക്ഷിക്കുന്നതിനുള്ള സുരക്ഷാ നടപടികൾ ഇതിൽ ഉൾപ്പെടുന്നു.
- വിവര സുരക്ഷ - ഇത് സ്വകാര്യത സംരക്ഷിക്കുന്നതിനും വിവരങ്ങളുടെ മോഷണം ഒഴിവാക്കുന്നതിനുമായുള്ള നടപടികളാണ്.
- ഡിസാസ്റ്റർ റിക്കവറി പ്ലാനിംഗ്- ഈ പ്രക്രിയയിൽ അപകടസാധ്യത വിലയിരുത്തൽ, ആക്രമണങ്ങൾക്കായി വീണ്ടെടുക്കൽ പദ്ധതികൾ വികസിപ്പിക്കൽ, മുൻഗണനകൾ സ്ഥാപിക്കൽ എന്നിവ ഉൾപ്പെടുന്നു.

ഇന്ത്യയിലെ സൈബർ നിയമങ്ങൾ

ഇത്തരം കുറ്റകൃത്യങ്ങൾ സംരക്ഷിക്കുന്നതിനും തടയുന്നതിനുമായി ഇന്ത്യയിൽ വിവിധ സൈബർ നിയമങ്ങളുണ്ട്.

ഇൻഫർമേഷൻ ടെക്നോളജി നിയമം, 2000

- 2020 ഒക്ടോബറിൽ നിലവിൽ വന്നു, ഇത് ഇന്ത്യൻ സൈബർ ആക്റ്റ് എന്നും അറിയപ്പെടുന്നു. എല്ലാ ഇ-ഇടപാടുകൾക്കും ഇത് നിയമപരമായ അംഗീകാരം നൽകുന്നു.

- ഇൻഫർമേഷൻ ടെക്നോളജി ആക്റ്റ് 2000 കമ്പ്യൂട്ടർ സിസ്റ്റങ്ങൾ, കമ്പ്യൂട്ടറുകൾ, കമ്പ്യൂട്ടർ നെറ്റ്‌വർക്കുകൾ, ഡാറ്റ, ഇലക്ട്രോണിക് ഫോർമാറ്റിലുള്ള വിവരങ്ങൾ എന്നിവയുടെ ഉപയോഗം നിയന്ത്രിക്കുന്നു.
- ഈ നിയമം ഇനിപ്പറയുന്ന കുറ്റങ്ങളായി പട്ടികപ്പെടുത്തുന്നു- ഒരു കമ്പ്യൂട്ടർ സിസ്റ്റം ഹാക്കിംഗ്, കമ്പ്യൂട്ടർ ഡോക്യുമെന്റുകളിൽ കൃത്രിമം കാണിക്കൽ, കമ്പ്യൂട്ടർ ഉറവിടങ്ങൾ ഉപയോഗിച്ച് വഞ്ചിക്കൽ, സൈബർ ഭീകരത തുടങ്ങിയ പ്രവൃത്തികൾ.

ദേശീയ സൈബർ നയം 2013

ദേശീയ സൈബർ നയം 2013 പ്രകാരമുള്ള തന്ത്രങ്ങൾ താഴെ പറയുന്നവയാണ്.

- ദേശീയ പ്രക്രിയകളിലൂടെയും സംവിധാനങ്ങളിലൂടെയും സുരക്ഷാ ഭീഷണികൾക്കും പ്രതികരണങ്ങൾക്കും സുരക്ഷിതമായ സൈബർ ആവാസവ്യവസ്ഥയും സംവിധാനങ്ങളും സൃഷ്ടിക്കുക.
- പബ്ലിക് കീ ഇൻഫ്രാസ്ട്രക്ചറിന്റെ ഉപയോഗവും മികച്ച രീതികളും നടപ്പിലാക്കുന്നതിലൂടെ ഇ-ഗവേണൻസ് സുരക്ഷിതമാക്കുക
- NCIIPC-യുമായുള്ള നിർണ്ണായക ഇൻഫർമേഷൻ ഇൻഫ്രാസ്ട്രക്ചറിന്റെ സംരക്ഷണം (NCIIPC-National Critical Information Infrastructure Protection Centre)
- പരിശീലനത്തിലൂടെയും വിദ്യാഭ്യാസ പരിപാടികളിലൂടെയും മാനവ വിഭവശേഷി വികസനം
- സൈബർ സുരക്ഷാ സാങ്കേതികവിദ്യകളുടെ വികസനം.

ദേശീയ സൈബർ സുരക്ഷാ തന്ത്രം 2020

ഇന്ത്യയിൽ സൈബർ ഇടം സുരക്ഷിതമാക്കാൻ നാഷണൽ സൈബർ സെക്യൂരിറ്റി സ്ട്രാറ്റജി 2020 നടപ്പിലാക്കാൻ ഇന്ത്യൻ സർക്കാർ പദ്ധതിയിട്ടിട്ടുണ്ട്.

സൈബർ സുരക്ഷിത് ഭാരത് ഇനിഷ്യേറ്റീവ്

MeitY ദേശീയ ഇ-ഗവേണൻസ് ഡിവിഷനുമായി (NeGD) സഹകരിച്ച് 2008-ൽ സൈബർ പ്രതിരോധശേഷിയുള്ള ഐടി സജ്ജീകരണം സ്ഥാപിക്കുന്നതിനായി ഈ സംരംഭം കൊണ്ടുവന്നു.

സൈബർ സുരക്ഷാ വെല്ലുവിളികൾ

ഇന്ത്യയിലെ സൈബർ സുരക്ഷ നിരവധി വെല്ലുവിളികൾ നേരിടുന്നു, അവ ഇനിപ്പറയുന്നവയാണ്

- ആളുകൾ മൊബൈൽ, ഇന്റർനെറ്റ് ഉപയോഗം വർധിച്ചു
- ചില ഉപകരണങ്ങളിൽ സോളിഡ് സെക്യൂരിറ്റി ഇൻഫ്രാസ്ട്രക്ചറിന്റെ അഭാവം

- ഇന്ത്യയിൽ സൈബർ സുരക്ഷയെക്കുറിച്ചുള്ള അവബോധമില്ലായ്മ
- തീവ്രവാദികളുടെ സൈബർസ്പേസ് ഉപയോഗം വർധിക്കുന്നു

ഇന്ത്യയിലെ സൈബർ സുരക്ഷ

ഇന്ത്യയിലെ സൈബർ സുരക്ഷയ്ക്കായി ഗവൺമെന്റ് അടുത്തിടെ എടുത്ത ചില സംരംഭങ്ങൾ ഇതാ.

ഇന്ത്യയിലെ സൈബർ സുരക്ഷയ്ക്കുള്ള സർക്കാർ സംരംഭങ്ങൾ	ലക്ഷ്യങ്ങൾ
സൈബർ സുരക്ഷിത് ഭാരത് ഇനിഷ്യേറ്റീവ്	2018-ൽ ആരംഭിച്ചത് സൈബർ കുറ്റകൃത്യങ്ങളെ കുറിച്ചുള്ള അവബോധം പ്രചരിപ്പിക്കുന്നതിനും സർക്കാർ വകുപ്പുകളിലുടനീളമുള്ള സിഐഎസ്ഒമാർക്കും (ചീഫ് ഇൻഫർമേഷൻ സെക്യൂരിറ്റി ഓഫീസർമാർ) ഫ്രണ്ട്ലൈൻ ഐടി ജീവനക്കാർക്കും വേണ്ടിയുള്ള സുരക്ഷാ നടപടികൾക്കുള്ള ശേഷി വർദ്ധിപ്പിക്കുന്നതിനും വേണ്ടിയാണ്.
നാഷണൽ സൈബർ സെക്യൂരിറ്റി കോർഡിനേഷൻ സെന്റർ (NCCC)	തത്സമയ സൈബർ ഭീഷണികൾ തടയുന്നതിനായി രാജ്യത്തേക്ക് വരുന്ന ഇന്റർനെറ്റ് ട്രാഫിക്കും കമ്മ്യൂണിക്കേഷൻ മെറ്റാഡാറ്റയും സ്കാൻ ചെയ്യുന്നതിനായി ഇത് 2019 ൽ ആരംഭിച്ചു.
സൈബർ സ്വച്ഛതാ കേന്ദ്രം	മാൽവെയറുകളും വൈറസുകളും തുടച്ചുനീക്കുന്നതിനായി ഇന്റർനെറ്റ് ഉപയോക്താക്കൾക്ക് അവരുടെ ഉപകരണങ്ങളും കമ്പ്യൂട്ടറും ക്ലിയർ ചെയ്യുന്നതിനായി ഈ പ്ലാറ്റ്ഫോം 2017 ൽ അവതരിപ്പിച്ചു.

ഇൻഫർമേഷൻ സെക്യൂരിറ്റി എഡ്യൂക്കേഷൻ ആൻഡ് അവയർനസ് പ്രോജക്ട് (ISEA)	സൈബർ സുരക്ഷാ മേഖലയിൽ അവബോധം വളർത്തുന്നതിനും വിദ്യാഭ്യാസം, ഗവേഷണം, പരിശീലനം എന്നിവ നൽകുന്നതിനുമായി ഈ പദ്ധതിക്ക് കീഴിൽ 52 സ്ഥാപനങ്ങളിലൂടെ 1.14 ലക്ഷം പേർക്ക് പരിശീലനം നൽകുന്നു.
അന്താരാഷ്ട്ര സഹകരണം	സൈബർ ആവാസവ്യവസ്ഥയെ ശക്തിപ്പെടുത്തുന്നതിനായി ജപ്പാൻ, യുണൈറ്റഡ് സ്റ്റേറ്റ്സ്, സിംഗപ്പൂർ തുടങ്ങിയ നിരവധി രാജ്യങ്ങളുമായി ഇന്ത്യ ചേർന്നു. സൈബർ ഭീഷണികളെ നേരിടുന്നതിൽ ഇന്ത്യയെ മികച്ചതാക്കാൻ ഇത് സഹായിക്കും.

സൈബർ സുരക്ഷയും സൈബർ ആക്രമണങ്ങളും

വർഷങ്ങളായി പരിണമിച്ച സൈബർ ആക്രമണങ്ങളുടെ തരങ്ങൾ താഴെ കൊടുക്കുന്നു

- **മാൽവെയർ**- ഒരു കമ്പ്യൂട്ടർ നെറ്റ്‌വർക്ക്, കമ്പ്യൂട്ടർ അല്ലെങ്കിൽ സെർവറിന് കേടുപാടുകൾ വരുത്താൻ മാത്രം രൂപകൽപ്പന ചെയ്തിരിക്കുന്ന ഏതെങ്കിലും തരത്തിലുള്ള സോഫ്റ്റ്‌വെയറിനെ മാൽവെയർ എന്ന് സൂചിപ്പിക്കുന്നു. വേമുകൾ, വൈറസുകൾ, സ്പൈവെയർ, ട്രോജനുകൾ എന്നിവ മാൽവെയറിന്റെ വകഭേദങ്ങളാണ്.
- വഞ്ചനാപരമായ ഇ-മെയിലുകളും വെബ്സൈറ്റുകളും ഉപയോഗിച്ച് വ്യക്തിഗത വിവരങ്ങൾ ശേഖരിക്കുന്ന രീതിയാണ് **Phishing**.
- **DOS, DDOS**- ആക്രമണകാരികൾ ഹോസ്റ്റ് നെറ്റ്‌വർക്കിന്റെ സേവനങ്ങൾ തടസ്സപ്പെടുത്തുന്നു.
- SQL Injection - സേവനങ്ങളുടെയും വെബ്സൈറ്റുകളുടെയും ഡാറ്റ സംഭരിക്കുന്ന പല സേവനദാതാക്കളും അവരുടെ ഡാറ്റാബേസുകൾ നിയന്ത്രിക്കാൻ SQL ഉപയോഗിക്കുന്നു. രഹസ്യാത്മക വിവരങ്ങൾ ലഭിക്കുന്നതിന് ക്ഷുദ്ര കോഡ് ഉപയോഗിച്ച് അത്തരം സെർവറുകളെ SQL ഇൻജക്ഷൻ ആക്രമണങ്ങൾ ലക്ഷ്യമിടുന്നു.
- സൈബർ ചാരവൃത്തി- രഹസ്യാത്മക വിവരങ്ങൾ പിടിച്ചെടുക്കാൻ കമ്പ്യൂട്ടർ നെറ്റ്‌വർക്കുകളുടെ നിയമവിരുദ്ധമായ ഉപയോഗം കാരണം ഒരു പ്രധാന സ്ഥാപനത്തിന്റെയോ സർക്കാരിന്റെയോ സ്വകാര്യത അപകടത്തിലാവുന്നു.
- സൈബർ യുദ്ധം- കമ്പ്യൂട്ടർ സാങ്കേതികവിദ്യ ഉപയോഗിച്ച്, പ്രത്യേകിച്ച് സൈനിക ആവശ്യങ്ങൾക്കായുള്ള വിവര സംവിധാനങ്ങളെ ആക്രമിക്കുന്നു.

- സോഷ്യൽ എഞ്ചിനീയറിംഗ്- സംരക്ഷിത സുപ്രധാന വിവരങ്ങൾ നേടുന്നതിന് ഉപയോക്താക്കളെ കബളിപ്പിക്കുക.

സൈബർ സുരക്ഷയ്ക്കുള്ള അന്താരാഷ്ട്ര സംവിധാനങ്ങൾ

- **ഇന്റർനാഷണൽ ടെലികമ്മ്യൂണിക്കേഷൻ യൂണിയൻ (ITU)-** സൈബർ സുരക്ഷയുടെയും ടെലികമ്മ്യൂണിക്കേഷൻ പ്രശ്നങ്ങളുടെയും വികസനത്തിലും സ്റ്റാൻഡേർഡൈസേഷനിലും സുപ്രധാന പങ്ക് വഹിക്കുന്ന ഐക്യരാഷ്ട്രസഭയിലെ ഒരു പ്രത്യേക ഏജൻസിയാണ്.
- **ബുഡാപെസ്റ്റ് കൺവെൻഷൻ ഓൺ സൈബർ ക്രൈം**- ദേശീയ നിയമങ്ങൾ യോജിപ്പിച്ച്, രാജ്യങ്ങൾ തമ്മിലുള്ള സഹകരണം വർദ്ധിപ്പിച്ച്, സൈബർ അന്വേഷണത്തിനുള്ള സാങ്കേതിക വിദ്യകൾ മെച്ചപ്പെടുത്തി സൈബർ കുറ്റകൃത്യങ്ങളെ അഭിസംബോധന ചെയ്യുന്ന ഒരു അന്താരാഷ്ട്ര സ്ഥാപനമാണ്.
- **ഇൻറർനെറ്റ് കോർപ്പറേഷൻ ഫോർ അസൈൻഡ് നെയിംസ് ആൻഡ് നമ്പേഴ്സ് (ICANN)**: സംഖ്യാ ഇടങ്ങളും നെയിംസ്പേസുകളും സംബന്ധിച്ച നിരവധി ഡാറ്റാബേസുകളുടെ പരിപാലനവും നടപടിക്രമങ്ങളും ഏകോപിപ്പിക്കുന്നതിനും സുരക്ഷിതമായ പ്രവർത്തനത്തിനായി നെറ്റ് വർക്കിന്റെ സ്ഥിരത ഉറപ്പാക്കുന്നതിനും ഉത്തരവാദിത്തമുള്ള ഒരു ലാഭേച്ഛയില്ലാത്ത സ്ഥാപനം.
- **ഇന്റർനെറ്റ് ഗവേണൻസ് ഫോറം (IGF)**- ഇന്റർനെറ്റ് ഭരണ സംവാദത്തിൽ സ്വകാര്യ മേഖല, സർക്കാർ, സിവിൽ സൊസൈറ്റി തുടങ്ങിയ എല്ലാ പങ്കാളികളെയും IGF ഒരുമിച്ച് കൊണ്ടുവരുന്നു..