15 –ാം കേരള നിയമസഭ

9 –ാം സമ്മേളനം

നക്ഷത്രചിഹ്നമിട്ട ചോദ്യം നം. 20 **08-08-2023 - ൽ മറുപടിയ്ക്ക്**

കമ്പ്യൂട്ടർ എമർജൻസി റെസ്പോൺസ് ടീം കേരള

ചോദ്യം		ഉത്തരം	
ശ്രീ. ആന്റണി ജോൺ, **ശ്രീ കെ യു ജനീഷ് കുമാർ,** **ശ്രീ. കെ. പ്രേംകുമാർ,** **ശ്രീ. എച്ച്. സലാം**		**ശ്രീ. പിണറായി വിജയൻ** **(മുഖ്യമന്ത്രി)**	
(എ)	സംസ്ഥാനത്തിന്റെ സമഗ്രമേഖലയിലും ഡിജിറ്റൽ സൗകര്യങ്ങൾ ഏർപ്പെടുത്തുകയും വ്യാപിപ്പിക്കുകയും ചെയ്യുമ്പോഴും സൈബർ കുറ്റകൃത്യങ്ങളും അതിക്രമങ്ങളും ഐ.ടി. മേഖലയെ ആശങ്കപ്പെടുത്തുന്നത് ഗൗരവമായി വിലയിരുത്തിയിട്ടുണ്ടോ;	(എ)	ഉണ്ട്. ഡിജിറ്റൽ സൗകര്യങ്ങൾ വർദ്ധിക്കുകയും അത് കൂടുതൽ ജനങ്ങളിലേക്ക് വ്യാപിക്കുകയും ചെയ്യുന്ന സാഹചര്യത്തിൽ ഇവയുടെ ഉപയോഗത്തിലും കാര്യക്ഷമതയിലും സൈബർ സുരക്ഷ ഉറപ്പുവരുത്തേണ്ടത് ആവശ്യമാണ്. ഇതോടൊപ്പം തന്നെ സാമൂഹിക മാധ്യമങ്ങൾ വഴി ഉണ്ടായേക്കാവുന്ന പല തരത്തിലുള്ള തട്ടിപ്പുകളുടെ പശ്ചാത്തലത്തിലും ഓൺലൈൻ സാമ്പത്തിക ക്രയ വിക്രയങ്ങളുടെ പശ്ചാത്തലത്തിലും വിവിധ തരത്തിൽ ശേഖരിച്ചിട്ടുള്ള ക്രിട്ടിക്കൽ ഇൻഫർമേഷൻ ചോർന്നു പോകാതെ സംരക്ഷിക്കുന്നതിനും ക്രിയാത്മകമായ സൈബർ സുരക്ഷ ഉറപ്പുവരുത്തേണ്ടതുണ്ട്. ഇത്തരത്തിലുള്ള കുറ്റകൃത്യങ്ങൾ ഫലപ്രദമായി നേരിടുന്നതിനുവേണ്ടി എല്ലാ പോലീസ് ജില്ലകളിലും (കണ്ണൂർ റൂറൽ ഒഴികെ) സൈബർക്രൈം പോലീസ് സ്റ്റേഷനുകൾ പ്രവർത്തിച്ചു വരുന്നു. സൈബർ മേഖലയിൽ സ്വകാര്യ പങ്കാളിത്തത്തോടെ ഗവേഷണം നടത്തുന്നതിനും സൈബർ വെല്ലുവിളികൾക്ക് സമയ ബന്ധിതമായി പരിഹാരം കാണുന്നതിനും തിരുവനന്തപുരം, കൊച്ചി, കോഴിക്കോട് എന്നീ സ്ഥലങ്ങൾ കേന്ദ്രീകരിച്ച് സൈബർ ഡോമുകൾ സ്ഥാപിച്ച് പ്രവർത്തിച്ചു വരുന്നു. സൈബർ മേഖലയിലുള്ള ചലനങ്ങൾ നിരീക്ഷിക്കുന്നതിനും നിർദ്ദേശങ്ങൾ രൂപവത്കരിക്കുന്നതിനും എസ്.പി. ടെക്നിക്കൽ ഇന്റലിജൻസ് എന്ന തസ്തിക സൃഷ്ടിച്ചിട്ടുണ്ട്. സൈബർ കുറ്റകൃത്യങ്ങളിൽ ക്രിയാത്മകമായ ഇടപെടൽ നടത്തുന്നതിനും സാങ്കേതിക നിർദ്ദേശങ്ങൾ നൽകുന്നതിനും കേന്ദ്രവും ഇതര സംസ്ഥാനങ്ങളുമായി ഏകോപന പ്രവർത്തനങ്ങൾ നടത്തുന്നതിനും ഐ.ജി. സൈബർ ഓപ്പറേഷൻസ്,

			എസ്.പി. സൈബർ ഓപ്പറേഷൻസ് എന്നീ തസ്തികകൾ സൃഷ്ടിച്ചിട്ടുണ്ട്. കൂടാതെ സൈബർ സുരക്ഷയും കുറ്റകൃത്യങ്ങളെയും സംബന്ധിച്ച് സുരക്ഷിതമായി ഓൺലൈൻ സങ്കേതങ്ങൾ ഉപയോഗിക്കുന്നതിനെ കുറിച്ചും സ്വീകരിക്കേണ്ട മുൻ കരുതലുകളെക്കുറിച്ചും സൈബർ പോലീസ് സ്റ്റേഷനുകൾ, ഹൈ-ടെക് ക്രൈം എൻക്വയറി സെൽ, സൈബർ ഡോം മുതലായവ വഴിയും കേരളാ പോലീസിന്റെ വിവിധ സോഷ്യൽ മീഡിയ പ്ലാറ്റ്ഫോമുകളിലൂടെയും ആവശ്യമായ ബോധവത്കരണം നിരന്തരം നടത്തി വരുന്നുണ്ട്. സൈബർ കുറ്റകൃത്യങ്ങളുടെ ഉറവിടത്തിന്റെ വലിയൊരു ശതമാനവും മറ്റ് സംസ്ഥാനങ്ങളിലാണെന്നുള്ള കാര്യം കൂടി പരിഗണിച്ച് കേന്ദ്ര സർക്കാരുമായി സഹകരിച്ച് സൈബർ കുറ്റകൃത്യങ്ങൾ തടയുന്നതിനും സൈബർ സുരക്ഷ ഉറപ്പുവരുത്തുന്നതിനും ഈ മേഖലയിലെ സാങ്കേതിക വളർച്ചയ്ക്ക് അനുസരിച്ചുള്ള ജാഗ്രതയും ഇടപെടലും നടത്തി സൈബർ കുറ്റാന്വേഷണം ത്വരിതപ്പെടുത്തുന്നതിനും വേണ്ട സത്വര നടപടികൾ സംസ്ഥാന പോലീസ് സ്വീകരിച്ചു വരുന്നു.
(ബി)	സൈബർ കുറ്റകൃത്യങ്ങളും അതിക്രമങ്ങളും തടയുന്നതിനായി എന്തെല്ലാം നൂതന സംവിധാനങ്ങളാണ് ഏർപ്പെടുത്തിയിരിക്കുന്നതെന്ന് വ്യക്തമാക്കുമോ;	(ബി)	• . സൈബർ കുറ്റകൃത്യങ്ങളും അതിക്രമങ്ങളും തടയുന്നതിനും സങ്കീർണ്ണമായ സൈബർ കുറ്റകൃത്യങ്ങൾ അന്വേഷിക്കുന്നതിനും വേണ്ടി എല്ലാ പോലീസ് ജില്ലകളിലും (കണ്ണൂർ റൂറൽ ഒഴികെ) സൈബർ പോലീസ് സ്റ്റേഷനുകൾ രൂപീകരിച്ചിട്ടുണ്ട്. സൈബർ പോലീസ് സ്റ്റേഷനുകളിൽ സൈബർ കുറ്റകൃത്യങ്ങൾ കൈകാര്യം ചെയ്യുന്നതിൽ വൈദഗ്ധ്യം നേടിയ പോലീസുകാരെ നിയോഗിച്ചിട്ടുള്ളതും സൈബർ ലോകത്തെ വെല്ലുവിളികൾ നേരിടുന്നതിനായി പോലീസുദ്യോഗസ്ഥർക്ക് സിഡാക്ക്, എൻസിആർബി എന്നിവിടങ്ങളിൽ പരിശീലനം നൽകി വരുന്നുണ്ട്. സൈബർ കുറ്റകൃത്യങ്ങളും അതിക്രമങ്ങളും തടയുന്നതിനായി രൂപീകരിച്ചിട്ടുള്ള കേരള സൈബർ ക്രൈം കോ-ഓർഡിനേഷൻ സെന്റർ (കെ 4 സി), ഇന്ത്യൻ സൈബർ ക്രൈം കോ-ഓർഡിനേഷൻ സെന്റർ (ഐ 4 സി) മായി സഹകരിച്ച് പ്രവർത്തിച്ച് വരുന്നു. രജിസ്റ്റർ ചെയ്ത കേസുകളുടെ അന്വേഷണത്തിനായി പരമാവധി നൂതന ഡിജിറ്റൽ എവിഡൻസ് കളക്ഷൻ ഉപകരണങ്ങളും ദ്രുതഗതിയിലുള്ള നടപടികൾ സ്വീകരിക്കുന്നതിനായി നാഷണൽ സൈബർ ക്രൈം റിപ്പോർട്ടിംഗ്

പോർട്ടലിന്റെ സേവനവും ഉപയോഗപ്പെടുത്തി വരുന്നുണ്ട്. 1930 എന്ന നമ്പരിൽ നിന്നും പോർട്ടൽ മുഖേന ഓൺലൈനായും പൊതുജനങ്ങൾക്ക് പരാതി ഫോൺ മുഖാന്തിരം അറിയിക്കാവുന്നതാണ്. സാമ്പത്തിക തട്ടിപ്പുകളുമായി ബന്ധപ്പെട്ട് അന്വേഷണ ഏജൻസികളും ബാങ്കുകൾ, ആർ ബി ഐ, സാമ്പത്തിക ഇടനിലക്കാർ, പേയ്മെന്റ്വാലറ്റുകൾ, എൻ പി സി ഐ (നാഷണൽ പേയ്മെന്റ്സ് കോർപ്പറേഷൻ ഓഫ് ഇന്ത്യ) മുതലായവ ഒരുമിച്ച് പ്രവർത്തിക്കുന്ന ഒരു പൊതു സംയോജിത പ്ലാറ്റ്ഫോമാണ് നാഷണൽ സൈബർ ക്രൈം റിപ്പോർട്ടിംഗ് പോർട്ടൽ. തട്ടിപ്പുകാരിലേക്ക് പോകുന്ന പണത്തിന്റെ ഒഴുക്ക് തടയുന്നതിന് സംസ്ഥാന പോലീസിന് ദ്രുതഗതിയിലുള്ള നടപടി സ്വീകരിക്കാൻ ഇതു വഴി കഴിയുന്നു.

-
- . സംസ്ഥാന സർക്കാരിന്റെ വിവിധ വകുപ്പുകളുടെ ഇ-ഗവേണൻസ് ആപ്ലിക്കേഷനുകൾ സുരക്ഷിതമായി കൈകാര്യം ചെയ്യുന്നതിനായി കേരള സംസ്ഥാന ഐ ടി മിഷൻറെ കീഴിൽ പ്രവർത്തിക്കുന്ന രണ്ടു ഡാറ്റാ സെന്ററുകളിലായി ഹോസ്റ്റ് ചെയ്തിരിക്കുന്നു. ഇങ്ങനെ ഹോസ്റ്റ് ചെയ്തിരിക്കുന്ന ആപ്ലിക്കേഷനുകളുടെ സുരക്ഷാ ഉറപ്പു വരുത്തുന്നതിനായി അത്യാധുനിക സംവിധാനങ്ങൾ സ്റ്റേറ്റ് ഡാറ്റാ സെന്ററുകളിൽ സജ്ജമാക്കിയിട്ടുണ്ട്.

. പുതുതായി രൂപകല്പന ചെയ്ത ഇ-ഗവേണൻസ് ആപ്ലിക്കേഷനുകൾ ഹോസ്റ്റ് ചെയ്യുന്നതിന് മുൻപായി സെക്യൂരിറ്റി ഓഡിറ്റ് നടത്തി ആപ്ലിക്കേഷനുകളിലെ സുരക്ഷാ ന്യൂനതകളെല്ലാം പരിഹരിച്ചു "സേഫ് ടു ഹോസ്റ്റ് സർട്ടിഫിക്കറ്റ്" സമർപ്പിച്ചെങ്കിൽ മാത്രമേ ഹോസ്റ്റ് ചെയ്യാനുള്ള തുടർനടപടിക്കായി അനുമതി ലഭിക്കുകയുള്ളു. ഇതിനു വേണ്ട മാർഗ്ഗ നിർദേശ രേഖകൾ സർക്കാർ പ്രസിദ്ധീകരിച്ചിട്ടുണ്ട്.

. സൈബർ ഇടം ശക്തിപ്പെടുത്തുന്നതിന് സംസ്ഥാന ഐടിമിഷനു കീഴിലുള്ള സെർട്ട്-കെ ദേശീയ സൈബർ കോർഡിനേഷൻ സെന്ററുമായി ചേർന്ന് പ്രവർത്തിച്ചുവരുന്നു.

. ഒരു മുൻകരുതൽ നടപടിയായി, നിലവിൽ ഹോസ്റ്റ് ചെയ്തിട്ടുള്ള ഇ-ഗവേണൻസ് ആപ്ലിക്കേഷനുകളുടെ

			സുരക്ഷാ ന്യൂനതകൾ സെർട്ട് - കെ പിരിയോഡിക്കലായി പരിശോധിച്ച കണ്ടെത്തുകയും , അതിലെ സുരക്ഷാ പാളിച്ചകൾ യഥാസമയം അതാത് വകുപ്പുകളെ അറിയിക്കുകയും വേണ്ട സുരക്ഷാ മാർഗ്ഗങ്ങൾ, നിർദ്ദേശങ്ങൾ എന്നിവ സെർട്ട് -കെ മുഖേന നൽകിവരുകയും ചെയ്യുന്നു.
(സി)	പുതുതായി ഉയർന്നുവരുന്ന സൈബർ ഭീഷണികളെ നേരിടുന്നതിന് പര്യാപ്തമാകും വിധം പ്രസ്തുത സംവിധാനങ്ങളെ വൈവിദ്ധ്യവൽക്കരിക്കുന്നതിന് നടപടി സ്വീകരിക്കുമോ;	(സി)	. സ്വീകരിച്ചുവരുന്നുണ്ട്. കാര്യക്ഷമമായ പോലീസിംഗിനുള്ള സാങ്കേതിക വിദ്യ വർദ്ധിപ്പിക്കുന്നതിലും സൈബർ ഇന്റലിജൻസ്, സൈബർ സെക്യൂരിറ്റി, ഇൻസിഡൻസ് റെസ്പോൺസ്, സൈബർസേഫ്റ്റി, ഡാർക്ക് നെറ്റ്/ വി.പി.എൻ മോണിറ്ററിംഗ് തുടങ്ങിയവ സൈബർഡോമിന്റെ ചില പ്രധാന പ്രവർത്തനങ്ങളാണ്. സ്റ്റുഡന്റ് പോലീസ് കേഡറ്റുകൾ, നാഷണൽ സർവ്വീസ് സ്കീം വോളന്റിയർമാർ, കോളേജ് സ്റ്റുഡന്റ്, റസിഡന്റ്സ് അസോസിയേഷനുകൾ മറ്റ് സർക്കാർ സ്ഥാപനങ്ങൾ എന്നിവർക്കായി നിരന്തരം സൈബർ ബോധവത്കരണ ക്ലാസ്/പ്രോഗ്രാമുകൾ നടത്തി ഓൺലൈൻ ചൂഷണങ്ങൾക്കെതിരായി പൊതുജനങ്ങളെ ബോധവത്കരിക്കുവാനുള്ള നടപടികൾ സംസ്ഥാന പോലീസ് സ്വീകരിച്ചു വരുന്നു. . ദേശീയ സൈബർ പ്രതിസന്ധികൾക്ക് പോലും കാരണമാകുന്ന സൈബർ ആക്രമണങ്ങൾക്ക് ഇരയാകാതിരിക്കാൻ നിർണായക വിവര സംവിധാനങ്ങൾ ഏറ്റവും ഉയർന്ന മുൻഗണനയോടെ സുരക്ഷിതമാക്കുകയും പരിരക്ഷിക്കുകയും വേണം. സൈബർ പ്രതിസന്ധിയിൽ നിന്ന് കരകയറുന്നതിനും പ്രതികരിക്കുന്നതിനും ഏകോപിപ്പിക്കുന്നതിനുമുള്ള ഒരു കർമ്മ പദ്ധതി തയ്യാറാക്കി നടപ്പിലാക്കേണ്ടതുണ്ട്. ഇതിൻറെ ഭാഗമായി ഒരു കരട് ആക്ഷൻ പ്ലാൻ തയ്യാറാക്കി വരികയാണ്. . ഇൻഫർമേഷൻ സെക്യൂരിറ്റി പോളിസി തയ്യാറാക്കുന്നതിനുള്ള നടപടികൾ സെർട്ട് -കെ സ്വീകരിച്ചു വരുന്നു. . സൈബർ സുരക്ഷാ അവബോധം ഫലപ്രദമായി കൂടുതൽ തലങ്ങളിലേക്ക് പ്രചരിപ്പിക്കുന്നതിനായി സ്കൂളുകൾ, കോളേജുകൾ, ജോലി സ്ഥലങ്ങൾ, വ്യവസായ തലങ്ങളിൽ ശിൽപശാലകൾ, വെബിനാറുകൾ, മത്സരങ്ങൾ എന്നിവയുടെ പരമ്പരകൾ നടത്താൻ സെർട്ട്-കെ പദ്ധതി തയ്യാറാക്കി വരുന്നു.
(ഡി)	നിലവിൽ സൈബർ ഭീഷണി നേരിടുന്നതിനായി	(ഡി)	സൈബർ സുരക്ഷയുമായി ബന്ധപ്പെട്ട വിഷയങ്ങൾ

കമ്പ്യൂട്ടർ എമർജൻസി റെസ്പോൺസ് ടീം കേരള (CERT-K)യുടെ നേതൃത്വത്തിൽ നടത്തിവരുന്ന പ്രവർത്തനങ്ങൾ എന്തെല്ലാമാണെന്ന് വിശദമാക്കുമോ?

കൈകാര്യം ചെയ്യുന്നതിനായി 2010 മെയ് മാസത്തിൽ കമ്പ്യൂട്ടർ എമർജൻസി റസ്പോൺസ് ടീം-കേരളയുടെ പ്രവർത്തനം ആരംഭിച്ചു. കമ്പ്യൂട്ടർ എമർജൻസി റെസ്പോൺസ് ടീം-ഇന്ത്യ (CERT-In) എന്ന വിഭാഗവുമായി CERT-K സഹകരിച്ചു പ്രവർത്തിക്കുന്നു.

<u>ചുമതലകൾ</u>

. സർക്കാർ വെബ്സൈറ്റുകളെ സൈബർ ആക്രമണങ്ങളിൽ നിന്നും പ്രതിരോധിക്കുന്നതിനായി സെർട്ട്-കെ വെബ്സൈറ്റുകളുടെ സുരക്ഷാ ഓഡിറ്റിംഗ് നടത്തുകയും, അതിലെ സുരക്ഷാ പാളിച്ചകൾ അതാത് വകുപ്പുകളെ അറിയിക്കുകയും അതിനു വേണ്ട സുരക്ഷാ മാർഗ്ഗങ്ങൾ നിർദ്ദേശിക്കുകയും ചെയ്തു വരുന്നു.

. സൈബർ സുരക്ഷാ ആക്രമണങ്ങൾക്ക് വിധേയമാകുന്ന സർക്കാർ വെബ്സൈറ്റ്/വെബ് ആപ്ലിക്കേഷന്റെ ഇൻസിഡന്റ്/ലോഗ് അനാലിസിസ് നടത്തുകയും ഭാവിയിൽ ഇത്തരത്തിലുള്ള ആക്രമണങ്ങൾ വരാതിരിക്കുവാൻ വേണ്ടിയുള്ള മുൻകരുതലുകൾ ആവിഷ്കരിക്കുകയും ചെയ്യുന്നു.

. വിവിധ വകുപ്പുകളിലുള്ള വിവര സാങ്കേതിക മേഖലയിലെ ഉദ്യോഗസ്ഥർക്ക് സൈബർ സെക്യൂരിറ്റി സംബന്ധമായ ബോധവൽക്കരണ ക്ലാസ്സുകൾ സംഘടിപ്പിക്കുകയും സുരക്ഷാ നിർദേശങ്ങൾ നല്കുകയും ചെയ്യുന്നു. കൂടാതെ സൈബർ സുരക്ഷയെ സംബന്ധിച്ച ബോധവൽക്കരണം സർക്കാർ ജീവനക്കാർ, പൊതുജനങ്ങൾ എന്നിവരിലേക്ക് പരമാവധി എത്തിക്കുക എന്ന ലക്ഷ്യത്തോടെ ഒരു ഓൺലൈൻ പോർട്ടൽ സജ്ജീകരിച്ചിട്ടുണ്ട്.

. ഓരോ ഓർഗനൈസേഷന്റെയും വകുപ്പുതല ചീഫ് ഇൻഫർമേഷൻ സെക്യൂരിറ്റി ഓഫീസർ (CISO) തിരിച്ചറിയുന്നതിനുള്ള നടപടികൾ ഇതിനകം തന്നെ ആരംഭിച്ചു കഴിഞ്ഞു.

. SDC/SECWAN എന്നിവയിലെ സെർവർ / നെറ്റ്വർക്കുകളുടെ സുരക്ഷാ വിടവുകൾ തിരിച്ചറിഞ്ഞു ക്രപാർശ ചെയ്യുന്നതിനായി ഇൻഫ്രാസ്ട്രക്ചർ ഓഡിറ്റ് നടത്തി സുരക്ഷ വർദ്ധിപ്പിക്കുന്നതിനുള്ള സുരക്ഷാ മാർഗ്ഗങ്ങൾ നിർദ്ദേശിക്കുകയും ചെയ്തു വരുന്നു.

. സൈബർ സ്വച്ഛതാ കേന്ദ്രം, NCIIPC, NIC-CERT മുതലായവയിൽ നിന്ന് ലഭിക്കുന്ന പ്രധാനപ്പെട്ട സൈബർ ഭീഷണി അലേർട്ടുകളും, CERT-IN പ്രസിദ്ധീകരിക്കുന്ന അഡ്വൈസറികളും, പ്രതിരോധ

			നടപടികളും അതാതു സർക്കാർ വകുപ്പുകൾക്കും, ഡാറ്റാസെന്ററുകൾക്കും നൽകി വരുന്നു. . സോഷ്യൽ മീഡിയ, ഡിജിറ്റൽ പേയ്മെന്റുകൾ തുടങ്ങിയവയുടെ ദ്രുതഗതിയിലും വ്യാപകവുമായ ഉപയോഗത്തെ കുറിച്ച് പൗരന്മാർക്കിടയിൽ അവബോധം സൃഷ്ടിക്കാൻ ലക്ഷ്യമിട്ട് ഇലക്ട്രോണിക്സ് ആൻഡ് ഇൻഫർമേഷൻ ടെക്നോളജി മന്ത്രാലയം (MeitY) 'സ്റ്റേ സേഫ് ഓൺലൈനിൽ' എന്ന പേരിൽ ഒരു ക്യാമ്പെയിൻ നടത്തിവരുന്നു. അതിന്റെ ഭാഗമായി ഒഫീഷ്യൽ സോഷ്യൽ മീഡിയ ഹാൻഡിലുകൾ വഴി അവബോധം നൽകിവരുന്നു. . സൈബർ ഇടം ശക്തിപ്പെടുത്തുന്നതിന് ദേശീയ സൈബർ കോർഡിനേഷൻ സെന്ററുമായി ചേർന്ന് പ്രവർത്തിച്ചുവരുന്നു.

സെക്ഷൻ ഓഫീസർ