

15 -ാം കേരള നിയമസഭ

10 -ാം സമ്മേളനം

നക്ഷത്ര ചിഹ്നം ഇല്ലാത്ത ചോദ്യം നം. 81

29-01-2024 - ൽ മറുപടിയ്ക്ക്

സൈബർ ആക്രമണങ്ങൾ തടയുന്നതിനുള്ള നടപടി

ചോദ്യം	ഉത്തരം
<p align="center"> ശ്രീ കെ യു ജനീഷ് കുമാർ, ശ്രീ എം.വിജിൻ, ശ്രീ സേവ്യർ ചിറ്റിലപ്പിള്ളി, ശ്രീ പി.വി. ശ്രീനിജിൻ </p>	<p align="center"> ശ്രീ. പിണറായി വിജയൻ (മുഖ്യമന്ത്രി) </p>
<p>(എ) സംസ്ഥാനത്ത് ഔദ്യോഗിക വെബ്സൈറ്റുകൾ ഹാക്കർമാരിൽ നിന്നും സംരക്ഷിക്കുന്നതിനാവശ്യമായ ജാഗ്രതാ നിർദ്ദേശം ബന്ധപ്പെട്ടവർക്ക് നൽകിയിട്ടുണ്ടോ; വിശദമാക്കുമോ;</p>	<p>(എ) കേരള പോലീസിന്റേത് ഉൾപ്പെടെ എല്ലാ സർക്കാർ വകുപ്പുകളിലെയും വെബ്സൈറ്റുകൾ സെക്യൂരിറ്റി ഓഡിറ്റ് നടത്തിയശേഷം സ്റ്റേറ്റ് ഡാറ്റാ സെന്ററിൽ ആണ് ഹോസ്റ്റ് ചെയ്യുന്നത്. ഈ വെബ്സൈറ്റുകൾ സ്റ്റേറ്റ് ഡാറ്റാ സെന്ററിൽ 24 X 7 പ്രവർത്തിക്കുന്ന സെക്യൂരിറ്റി ഓപ്പറേഷൻ സെന്ററിൽ (SOC) സസൃഷ്ടം നിരീക്ഷണത്തിലാണ്. കൂടാതെ കമ്പ്യൂട്ടർ എമർജൻസി റെസ്പോൺസ് ടീം ഇന്ത്യ (CERT-IN), നാഷണൽ സൈബർ കോ-ഓഡിനേഷൻ സെന്റർ (NCCC), നാഷണൽ ക്രിട്ടിക്കൽ ഇൻഫർമേഷൻ ഇൻഫ്രാസ്ട്രക്ചർ പ്രൊട്ടക്ഷൻ സെന്റർ (NCIIPC) എന്നിവിടങ്ങളിൽ നിന്നും ലഭിക്കുന്ന വശ്നറബിലിറ്റി അസസ്സ്മെന്റ് റിപ്പോർട്ട് പരിശോധിച്ച് പോലീസ് വകുപ്പ്, കമ്പ്യൂട്ടർ എമർജൻസി റെസ്പോൺസ് ടീം കേരളയുമായി (CERT-K) കൂടിയാലോചിച്ച് മുൻകരുതൽ നടപടികൾ സ്വീകരിച്ചു വരുന്നു. കൂടാതെ സർക്കാർ വെബ്സൈറ്റുകളെ സൈബർ ആക്രമണങ്ങളിൽ നിന്നും പ്രതിരോധിക്കുന്നതിനായി സെർട്ട്-കെ ചുവടെ പറയുന്ന പ്രവർത്തനങ്ങൾ നടത്തിവരുന്നു.</p> <p>പുതുതായി രൂപകല്പന ചെയ്ത ഇ-ഗവേണൻസ് ആപ്ലിക്കേഷനുകൾ ഹോസ്റ്റ് ചെയ്യുന്നതിന് മുൻപായി സെക്യൂരിറ്റി ഓഡിറ്റ് നടത്തി അപ്ലിക്കേഷനുകളിലെ സുരക്ഷാ ന്യൂനതകളെല്ലാം പരിഹരിച്ചു "സേഫ് ടു ഹോസ്റ്റ് സർട്ടിഫിക്കറ്റ്" സമർപ്പിച്ചെങ്കിൽ മാത്രമേ ഹോസ്റ്റ് ചെയ്യാനുള്ള തുടർനടപടിക്കായി അനുമതി ലഭിക്കുകയുള്ളൂ. ഇതിനു വേണ്ട മാർഗ നിർദ്ദേശ രേഖകൾ ഐ.ടി വകുപ്പ് പ്രസിദ്ധീകരിച്ചിട്ടുണ്ട്.</p> <p>ഒരു മുൻകരുതൽ നടപടിയായി, നിലവിൽ ഹോസ്റ്റ് ചെയ്തിട്ടുള്ള ഇ-ഗവേണൻസ് ആപ്ലിക്കേഷനുകളുടെ</p>

		<p>സുരക്ഷാ ന്യൂനതകൾ സെർട്ട് - കെ പിരിയോഡിക്കലായി പരിശോധിച്ചു കണ്ടെത്തുകയും, അതിലെ സുരക്ഷാ പാളിച്ചകൾ യഥാസമയം അതാത് ഡിപ്പാർട്ടുമെന്റുകളെ അറിയിക്കുകയും വേണ്ട സുരക്ഷാ മാർഗ്ഗനിർദ്ദേശങ്ങൾ നൽകിവരുകയും ചെയ്യുന്നു.</p> <p>സൈബർ സുരക്ഷാ ആക്രമണങ്ങൾക്ക് വിധേയമാകുന്ന സർക്കാർ വെബ്സൈറ്റ്/വെബ് അപ്ലിക്കേഷന്റെ ഇൻസിഡന്റ്/ലോഗ് അനാലിസിസ് നടത്തുകയും ഭാവിയിൽ ഇത്തരത്തിലുള്ള ആക്രമണങ്ങൾ വരാതിരിക്കുവാൻ വേണ്ടിയുള്ള മുൻകരുതലുകൾ ആവിഷ്കരിക്കുകയും ചെയ്യുന്നു.</p> <p>വിവിധ ഡിപ്പാർട്ടുമെന്റിലുള്ള വിവര സാങ്കേതിക മേഖലയിലെ ഉദ്യോഗസ്ഥർക്ക് സൈബർ സെക്യൂരിറ്റി സംബന്ധമായ ബോധവൽക്കരണ ക്ലാസ്സുകൾ സംഘടിപ്പിക്കുകയും സുരക്ഷാ നിർദ്ദേശങ്ങൾ നൽകുകയും ചെയ്യുന്നു. കൂടാതെ സൈബർ സുരക്ഷയെ സംബന്ധിച്ച ബോധവൽക്കരണം സർക്കാർ ജീവനക്കാർ, പൊതുജനങ്ങൾ എന്നിവരിലേക്ക് പരമാവധി എത്തിക്കുക എന്ന ലക്ഷ്യത്തോടെ ഒരു ഓൺലൈൻ പോർട്ടൽ സജ്ജീകരിച്ചിട്ടുണ്ട്.</p>
(ബി)	<p>അമേരിക്ക കേന്ദ്രീകരിച്ചുള്ള ഹാക്കർമാരുടെ സൈബർ ആക്രമണത്തിൽ നിന്ന് കേരള പോലീസിന്റെ കമ്പ്യൂട്ടർ ശൃംഖലയെ സംരക്ഷിക്കുന്നതിൽ നടത്തിയ സമയോചിത ഇടപെടൽ ഫലപ്രദമായിട്ടുണ്ടോ; അറിയിക്കുമോ;</p>	<p>(ബി) കേരള പോലീസിന്റെ കമ്പ്യൂട്ടറുകളും കമ്പ്യൂട്ടർ നെറ്റ് വർക്കുകളും സംരക്ഷിക്കുന്ന ചുമതലകൾക്കായി സൈബർ ഓപ്പറേഷൻ പോലീസ് ഇൻസ്പെക്ടർ ജനറലിനെ ചീഫ് ഇൻഫർമേഷൻ സെക്യൂരിറ്റി ഓഫീസറായും (CISO) സൈബർ ഓപ്പറേഷൻസ് പോലീസ് സൂപ്രണ്ട്, ടെക്നിക്കൽ ഇൻലിജൻസ് പോലീസ് സൂപ്രണ്ട്, ടെലി കമ്മ്യൂണിക്കേഷൻ & ടെക്നോളജി പോലീസ് സൂപ്രണ്ട് എന്നീ ഉദ്യോഗസ്ഥരെ ഡെപ്യൂട്ടി ചീഫ് ഇൻഫർമേഷൻ സെക്യൂരിറ്റി ഓഫീസർമാരായും നിയമിച്ചിട്ടുണ്ട്. ചീഫ് ഇൻഫർമേഷൻ സെക്യൂരിറ്റി ഓഫീസിന്റെ നിയന്ത്രണത്തിൽ കമ്പ്യൂട്ടർ എമർജൻസി റെസ്പോൺസ് ടീം കേരളയുടെയും (CERT-K) കേരള പോലീസിന്റെ ഡിസ്ട്രിക്ട് കമ്പ്യൂട്ടർ മെയിന്റനൻസ് യൂണിറ്റിന്റെയും (DCMU) പ്രവർത്തനങ്ങൾ ഏകോപിപ്പിച്ച് ഇൻസിഡന്റ് റെസ്പോൺസ് ടീമായി പ്രവർത്തിക്കുന്ന സൈബർ സെക്യൂരിറ്റി ഡെസ്ക് സൈബർ ഓപ്പറേഷൻ ആസ്ഥാനത്ത് പ്രവർത്തനം ആരംഭിച്ചിട്ടുണ്ട്. കേരള പോലീസിന്റെ നെറ്റ് വർക്കും കമ്പ്യൂട്ടറുകളും സമ്പൂർണ്ണ സംരക്ഷണ വലയത്തിൽ കൊണ്ടു വരുന്നതിലേക്കായി വകുപ്പ് തലത്തിൽ ഒരു ഉപ സെക്യൂരിറ്റി ഓപ്പറേഷൻ സെന്റർ (Sub SOC)</p>

		<p>രൂപകൽപ്പന ചെയ്യുന്ന നടപടികൾ സെൻട്രൽ ഫോർ ഡെവലപ്മെന്റ് ഓഫ് ടെലിമാറ്റിക്സുമായി (CDOT) സഹകരിച്ച് ദൃഢഗതിയിൽ നടന്നു വരുന്നു. പോലീസ് സേനയെ സൈബർ അറ്റാക്കുകൾ നേരിടാൻ സുസജ്ജമാക്കുന്നതിന്റെ ഭാഗമായി ഒരു വിദഗ്ദ്ധസേനയെ സംസ്ഥാന തലത്തിലും ജില്ലാ തലത്തിലും രൂപീകരിക്കുവാൻ വേണ്ടി ബി.എസ്.എൻ.എൽ, കൊച്ചിൻ യൂണിവേഴ്സിറ്റി ഓഫ് സയൻസ് ആൻഡ് ടെക്നോളജി (CUSAT), ഇന്ത്യൻ ഇൻസ്റ്റിറ്റ്യൂട്ട് ഓഫ് ഇൻഫർമേഷൻ ടെക്നോളജി (IIIT), നാഷണൽ ഫോറൻസിക് സയൻസ് യൂണിവേഴ്സിറ്റി (NFSU) എന്നീ ഏജൻസികളുമായി ചേർന്ന് സമഗ്രമായ പരിശീലന പരിപാടികൾ നടത്തി വരുന്നു. പോലീസിന്റെ കമ്പ്യൂട്ടർ നെറ്റ് വർക്ക് സുരക്ഷിതമാക്കുന്നതിനായി ഫോർട്ടി ക്ലൈന്റ് സോഫ്റ്റ് വെയർ ഉപയോഗിക്കുന്നുണ്ട്. കൂടാതെ മിനിസ്ട്രി ഓഫ് ഹോം അഫേയ്സിന്റെ കീഴിലുള്ള ഇൻഡ്യൻ സൈബർ ക്രൈം കോ-ഓർഡിനേഷൻ സെന്റർ, മിനിസ്ട്രി ഓഫ് ഇലക്ട്രോണിക് & ഇൻഫർമേഷൻ ടെക്നോളജിയ്ക്ക് കീഴിലുള്ള കമ്പ്യൂട്ടർ എമർജൻസി റെസ്പോൺസ് ടീം എന്നിവയുടെ നിർദ്ദേശങ്ങളും ഹാക്കിംഗിനെ ഫലപ്രദമായി നേരിടാൻ ഉപയോഗപ്പെടുത്തുന്നുണ്ട്.</p>
<p>(സി) ഇത്തരത്തിലുള്ള സൈബർ അറ്റാക്കുകൾ തടയുന്നതിനും വെബ്സൈറ്റുകൾ സംരക്ഷിക്കുന്നതിനും മറ്റ് ഔദ്യോഗിക ഏജൻസികളുടെ സഹകരണം സംസ്ഥാന പോലീസിന് ലഭ്യമാക്കാൻ വിവര സാങ്കേതികവിദ്യാ വകുപ്പിന് കഴിഞ്ഞിട്ടുണ്ടോ; വ്യക്തമാക്കുമോ;</p>	<p>(സി) സൈബർ അറ്റാക്കുകൾ തടയുന്നതിനും വെബ്സൈറ്റുകൾ സംരക്ഷിക്കുന്നതിനുമായി കേരളത്തിലെ മറ്റ് ഔദ്യോഗിക ഏജൻസികളായ സെന്റർ ഫോർ ഡെവലപ്മെന്റ് ഓഫ് അഡ്വാൻസ്ഡ് കമ്പ്യൂട്ടിംഗ് (C-DAC), കമ്പ്യൂട്ടർ എമർജൻസി റെസ്പോൺസ് ടീം കേരള (CERT-K), കേരള സ്റ്റേറ്റ് ഇലക്ട്രോണിക് ഡെവലപ്മെന്റ് കോർപ്പറേഷൻ (KELTRON) എന്നീ ഏജൻസികളുടെ സഹകരണം സംസ്ഥാന പോലീസിന് ലഭ്യമാക്കുന്നതിന് വിവര സാങ്കേതികവിദ്യാ വകുപ്പിന് കഴിഞ്ഞിട്ടുണ്ട്. കമ്പ്യൂട്ടർ എമർജൻസി റെസ്പോൺസ് ടീം കേരള(CERT-K)-യുമായി നിരന്തര സമ്പർക്കം പുലർത്തിയാണ് സൈബർ ഓപ്പറേഷൻ ആസ്ഥാനത്ത് പ്രവർത്തിച്ചു വരുന്ന സൈബർ സെക്യൂരിറ്റി ഡെസ്ക് മുഖാന്തിരം ചീഫ് ഇൻഫർമേഷൻ സെക്യൂരിറ്റി ഓഫീസർ (CISO) നടപടികൾ സ്വീകരിച്ചു വരുന്നത്. കമ്പ്യൂട്ടർ എമർജൻസി റെസ്പോൺസ് ടീം കേരള (CERT-K) കേന്ദ്ര ഏജൻസികളായ ഇന്ത്യൻ സൈബർ ക്രൈം കോർഡിനേഷൻ സെന്റർ (ICCCC), നാഷണൽ സൈബർ കോർഡിനേഷൻ സെന്റർ (NCCC), നാഷണൽ ക്രിട്ടിക്കൽ ഇൻഫർമേഷൻ ഇൻഫ്രാസ്ട്രക്ചർ പ്രൊട്ടക്ഷൻ സെന്റർ (NCIIPC),</p>	

		<p>സൈബർ സ്വച്ഛതാ കേന്ദ്രം, കമ്പ്യൂട്ടർ എമർജൻസി റെസ്പോൺസ് ടീം ഇന്ത്യ (CERT-IN) എന്നിവയുമായി നിരന്തര സമ്പർക്കം പുലർത്തിക്കൊണ്ട് സൈബർ സുരക്ഷയുമായി ബന്ധപ്പെട്ട വിഷയങ്ങളിൽ സംസ്ഥാന പോലീസ് ഉൾപ്പെടെയുള്ള വകുപ്പുകൾക്ക് സഹായ സഹകരണങ്ങൾ എത്തിച്ചു നൽകുകയും അവരുമായി ചേർന്നു പ്രവർത്തിക്കുകയും ചെയ്യുന്നുണ്ട്.</p>
<p>(ഡി) സംസ്ഥാന സൈബർ പോലീസിന് അത്യാധുനിക സാങ്കേതികവിദ്യയിൽ ആവശ്യമായ പരിശീലനം നൽകാൻ നടപടി സ്വീകരിക്കുമോ?</p>		<p>(ഡി) സംസ്ഥാനത്ത് പോലീസ് ഉദ്യോഗസ്ഥർക്ക് സൈബർ സൈക്യൂരിറ്റി, ഡാർക്ക് വെബ് തുടങ്ങിയ വിഷയങ്ങളിൽ പരിശീലനം നൽകി വരുന്നതും, തെരഞ്ഞെടുക്കപ്പെട്ട സേനാംഗങ്ങൾക്ക് സെന്റർ ഫോർ ഡവലപ്പ്മെന്റ് ഓഫ് അഡ്വാൻസ്ഡ് കമ്പ്യൂട്ടിംഗ് (C-DAC), കേരള പോലീസ് അക്കാദമി (KEPA), സെന്റർ ഫോർ ഡവലപ്പ്മെന്റ് ഓഫ് ഇമേജിംഗ് ട്രെയിനിംഗ് സെന്റർ (C-DIT), സെൻട്രൽ ഡിറ്റക്ടിവ് ട്രെയിനിംഗ് ഇൻസ്റ്റിറ്റ്യൂട്ട് (CDTI), നാഷണൽ ക്രൈം റിക്വോർഡ്സ് ബ്യൂറോ (NCRB), നാഷണൽ സൈബർ ക്രൈം ട്രെയിനിംഗ് സെന്റർ (CyTrain), സൈബർ ക്രൈം ഇൻവെസ്റ്റിഗേഷൻ ട്രെയിനിംഗ് & റിസർച്ച് (CCITR) ബാംഗ്ലൂർ, നാഷണൽ ടെക്നിക്കൽ & റിസർച്ച് ഓർഗനൈസേഷൻ (NTRO) ന്യൂഡെൽഹി എന്നിവിടങ്ങളിൽ അയച്ച് പ്രത്യേക പരിശീലനം നൽകി വരുന്നു. കൂടാതെ പോലീസ് ട്രെയിനിംഗ് കോളേജിൽ Tracking of Cyber Crime and Empowering the Cyber Arms of Kerala Police എന്നൊരു പരിശീലന പരിപാടി നടന്ന് വരുന്നുണ്ട്. സൈബർ സൈക്യൂരിറ്റി, എത്തിക്കൽ ഹാക്കിംഗ്, നെറ്റ് വർക്ക് സുരക്ഷ, റിസ്ക് മാനേജ്മെന്റ്, ഡിജിറ്റൽ ഫോറൻസിക് തുടങ്ങിയ മേഖലകളിൽ സാങ്കേതിക വശം മെച്ചപ്പെടുത്തുന്നതിനും, ഓൺലൈൻ സാമ്പത്തിക കുറ്റകൃത്യങ്ങൾ തടയുന്നതിനും പുതുതായി പോലീസ് ആസ്ഥാനം കേന്ദ്രമാക്കി സൈബർ ഡിവിഷൻ (സൈബർ ഓപ്പറേഷൻ, റിസർച്ച് അനാലിസിസ് യൂണിറ്റ്) ആരംഭിച്ചിട്ടുള്ളതും, സംസ്ഥാനത്ത് സൈബർ കുറ്റകൃത്യങ്ങൾ തടയാൻ എല്ലാ പോലീസ് ജില്ലകളിലും (കണ്ണൂർ റൂറൽ ഒഴികെ) സൈബർ പോലീസ് സ്റ്റേഷൻ രൂപീകരിച്ചിട്ടുള്ളതും ടി യൂണിറ്റുകളിൽ സാങ്കേതിക പരിജ്ഞാനമുള്ള ഉദ്യോഗസ്ഥരെ നിയമിച്ചിട്ടുള്ളതുമാണ്. കൂടാതെ പോലീസ് സ്റ്റേഷൻ തലത്തിൽ കേസ് അന്വേഷണത്തിന് അടിയന്തിര സഹായം ലഭ്യമാക്കുന്നതിനായി 3 പോലീസുകാർ ഉൾപ്പെട്ട സൈബർ ഫോറൻസിക് ടീം രൂപീകരിച്ച് അവർക്ക് പരിശീലനം നൽകിയിട്ടുള്ളതുമാണ്. സംസ്ഥാന</p>

പോലീസ് സേനയിലെ 25 പോലീസ് ഉദ്യോഗസ്ഥർക്ക് ഡാർക്ക് വെബ് മേഖലയിലും, 75 പോലീസ് ഉദ്യോഗസ്ഥർക്ക് സൈബർ സെക്യൂരിറ്റി മേഖലയിലും, 50 പോലീസ് ഉദ്യോഗസ്ഥർക്ക് ക്രിപ്റ്റോ കറൻസിയിലും പ്രമുഖ ഏജൻസികൾ മുഖാന്തരം അത്യധുനിക പരിശീലനം നൽകിയിട്ടുള്ളതും, ഗവൺമെന്റ് ഓഫ് ഇന്ത്യയുടെ നിർദ്ദേശാനുസരണം സംസ്ഥാന പോലീസിൽ നിന്നും തിരഞ്ഞെടുക്കപ്പെട്ട 20 സബ് ഇൻസ്പെക്ടർമാരെ ഉൾപ്പെടുത്തി സൈബർ കമാൻഡോ വിഭാഗം രൂപീകരിച്ചിട്ടുള്ളതുമാണ്. ഇത് കൂടാതെ സംസ്ഥാന പോലീസ് സേനയിലെ 360 ഓഫീസർമാർ ഉൾപ്പെടെ 860 പോലീസ് ഉദ്യോഗസ്ഥർ സൈബർ കുറ്റകൃത്യങ്ങൾ അന്വേഷിക്കുവാനും തടയുവാനും വേണ്ടിയുള്ള അടിസ്ഥാന പരിശീലനം പൂർത്തിയാക്കിയിട്ടുള്ളതുമാണ്.

സെക്ഷൻ ഓഫീസർ