15 -ാം കേരള നിയമസഭ

11 -ാം സമ്മേളനം

നക്ഷത്രചിഹ്നമിട്ട ചോദ്യം നം. 454 **08-07-2024 - ൽ മറുപടിയ്ക്ക്**

ആർ.സി.സി.യിലെ സൈബർ ആക്രമണം

ചോദ്യം		ഉത്തരം	
ശ്രീമതി കെ. കെ. രമ, ശ്രീ. എ. പി. അനിൽ കുമാർ , ശ്രീ. സി. ആർ. മഹേഷ്, ശ്രീ. ടി. സിദ്ദിഖ്		ശ്രീമതി വീണാ ജോർജ്ജ് (ആരോഗ്യ- വനിത-ശിശുവികസന വകുപ്പ് മന്ത്രി)	
(എ)	റീജിയണൽ ക്യാൻസർ സെന്ററിൽ റേഡിയേഷൻ ചികിത്സയ്ക്കുള്ള സോഫ്റ്റ്‌വെയറിലടക്കം വിദേശ സൈബർ ആക്രമണം നടന്നത് ശ്രദ്ധയിൽപ്പെട്ടിട്ടുണ്ടോ;	(എ)	സൈബർ ആക്രമണം നടന്നിട്ടുണ്ട്.
(ബി)	റേഡിയേഷൻ ചികിത്സയ്ക്കുള്ള സോഫ്റ്റ്‌വെയർ, ഇരുപത് ലക്ഷത്തിലേറെ രോഗികളുടെ ആരോഗ്യവിവരങ്ങളടക്കം സൂക്ഷിച്ചിട്ടുള്ള രണ്ട് പ്രധാന സെർവറുകൾ എന്നിവ ഹാക്ക് ചെയ്യപ്പെട്ടു എന്നത് പരിശോധിച്ചിട്ടുണ്ടോ; എങ്കിൽ ഇക്കാര്യത്തിൽ സ്വീകരിച്ച നടപടികൾ വിശദമാക്കുമോ;?	(ബി)	റീജിയണൽ കാൻസർ സെന്ററിലെ റേഡിയോ ഡയഗ്നോസിസ് വിഭാഗത്തിലെ M/s GE കമ്പനിയുടെ PACS സോഫ്റ്റ് വെയറിലും റേഡിയേഷൻ ഫിസിക്സ് വിഭാഗത്തിലെ M/s VARIAN കമ്പനിയുടെ CITRIX സോഫ്റ്റ് വെയറിലും ആണ് 28/04/2024 - ന് സൈബർ ആക്രമണം ഉണ്ടായത്. പക്ഷെ ക്രിട്ടിക്കൽ സിസ്റ്റത്തിൽ ബാധിക്കുന്നതിനു മുൻപ് തന്നെ അത് കണ്ടെത്തുകയും അതിന്റെ പ്രവർത്തനം നിർത്തി വയ്ക്കുകയും ചെയ്തു. സൈബർ ആക്രമണം കണ്ടെത്തിയതിന്റെ ആദ്യ ദിനം മുതൽ തന്നെ അതിനെ മറ്റു കംപ്യൂട്ടറുകളിൽ വ്യാപിക്കാതിരിക്കാനുള്ള നടപടികൾ RCC സ്വീകരിച്ചിരുന്നു. തുടർന്ന് അടിയന്തരമായി സർക്കാരിനെയും സൈബർ സെക്യൂരിറ്റി വിഭാഗത്തെയും സെർട്ടിനെയും (Computer Emergency Response Team, Kerala) അറിയിക്കുകയും ആരോഗ്യ വകുപ്പ് മന്ത്രിയുടെയും വിദഗ്ധ സമിതിയുടെയും നേതൃത്വത്തിൽ നടത്തിയ ചർച്ചയുടെ അടിസ്ഥാനത്തിൽ ആർസി സി യിൽ നിന്നും 29/04/2024-ന് ഔദ്യോഗികമായി Superintendent of Police, Cyber Operations ന് പരാതി നൽകുകയും അവരുടെ നിർദേശപ്രകാരം 08/05/2024 ന് തിരുവനന്തപുരം പോലീസ് കമ്മീഷണർക്ക് പരാതി നൽകിയതിന്റെ അടിസ്ഥാനത്തിൽ 09/05/2024-ന് സൈബർ ക്രൈം വിഭാഗം 0116/2024 നമ്പറായി FIR രജിസ്റ്റർ ചെയ്യുകയും ചെയ്തു.

			സൈബർ വിഭാഗവും സെർട്ടും അനാലിസിസ് നടത്തിയതിന്റെ അടിസ്ഥാനത്തിൽ 8 ഡെസ്ക്ക് ടോപ് പിസികളിലും 4 സെർവറുകളിലും ആണ് വൈറസ് ബാധിച്ചതെന്ന് കണ്ടുപിടിക്കുകയും തുടർന്ന് ഇൻഫെക്ടഡ് ആയിട്ടുള്ള കംപ്യൂട്ടറുകളിലുള്ള വിവരങ്ങൾ പുനഃസ്ഥാപിക്കുന്നതിനു വേണ്ടി 5 ദിവസം സ്ഥാപനത്തിലെ രോഗികളുടെ ചികിത്സ നിർത്തി വയ്ക്കുകയും ആറാം ദിനം പുനരാരംഭി-ക്കുകയും ചെയ്തു. സൈബർ ആക്രമണം നേരിട്ട മറ്റു കംപ്യൂട്ടറുകൾ സൈബർ വിഭാഗവും CERT ഉം തുടർ പരിശോധനകൾക്കായി ഏറ്റെടുത്തിട്ടുണ്ട്. സൈബർ വിഭാഗത്തിന്റെയും സെർട്ടിന്റെയും നിർദ്ദേശപ്രകാരം രോഗികളുടെ ചികിത്സാ രേഖകൾക്ക് കൂടുതൽ സുരക്ഷ ഉറപ്പാക്കുന്നതിനും ഭാവിയിൽ ഇത്തരം സൈബർ ആക്രമണങ്ങൾ വരാതിരിക്കുന്നതിനും ഉള്ള നടപടികൾ RCC സ്വീകരിച്ചു വരികയാണ്. ബാക്കപ്പ് ഉള്ളതിനാൽ രോഗികളുടെ റേഡിയേഷൻ ചികിത്സ വിവരങ്ങൾ സുരക്ഷിതവുമാണ്.

സെക്ഷൻ ഓഫീസർ