15 -ാം കേരള നിയമസഭ

11 -ാം സമ്മേളനം

നക്ഷത്ര ചിഹ്നം ഇല്ലാത്ത ചോദ്യം നം. 5731 **08-07-2024 - ൽ മറുപടിയ്ക്ക്**

ആർ.സി.സി.യിലെ സൈബർ ആക്രമണം

ചോദ്യം		ഉത്തരം	
ശ്രീ. തിരുവഞ്ചൂർ രാധാകൃഷ്ണൻ		ശ്രീമതി വീണാ ജോർജ്ജ് (ആരോഗ്യ- വനിത-ശിശുവികസന വകുപ്പ് മന്ത്രി)	
(എ)	ആർ.സി.സി.യിൽ നടന്ന സൈബർ ആക്രമണത്തിലൂടെ രോഗികളുടെ ആരോഗ്യവിവരങ്ങൾ ചോർന്നത് ഗൗരവത്തോടെ കാണുന്നുണ്ടോ; ഏതെല്ലാം സോഫ്റ്റ്‌വെയറുകളിലാണ് സൈബർ ആക്രമണം നേരിട്ടതെന്നും പ്രസ്തുത ഗുരുതര പ്രതിസന്ധി പരിഹരിക്കുന്നതിനായി സ്വീകരിച്ച നടപടികളും വ്യക്തമാക്കുമോ;	(എ)	റീജിയണൽ കാൻസർ സെന്ററിൽ 28/04/2024—നു 08.42 PM-നു റേഡിയോ ഡയഗ്നോസിസ് വിഭാഗത്തി ലെ M/s GE കമ്പനിയുടെ PACS സോഫ്റ്റ് വെയറിലും റേഡിയേഷൻ ഫിസിക്സ് വിഭാഗത്തിലെ M/s VARIAN കമ്പനിയുടെ CITRIX സോഫ്റ്റ് വെയറിലും ആണ് സൈബർ ആക്രമണം നേരിട്ടത്. പക്ഷെ ക്രിട്ടിക്കൽ സിസ്റ്റത്തിൽ ബാധിക്കുന്നതിനു മുൻപ് തന്നെ സൈബർ ആക്രമണം തിരിച്ചറിയുകയും അതിന്റെ പ്രവർത്തനം നിർത്തി വയ്ക്കുകയും ചെയ്തു. സൈബർ ആക്രമണം കണ്ടെത്തിയതിന്റെ ആദ്യ ദിനം മുതൽ തന്നെ വൈറസ് മറ്റു കംപ്യൂട്ടറുകളിൽ വ്യാപിക്കാതിരിക്കാനുള്ള നടപടികൾ RCC സ്വീകരിച്ചിരുന്നു. തുടർന്ന് അടിയന്തരമായി 29/04/2024-തീയതിയിൽ തന്നെ സർക്കാരിനെയും സൈബർ സെക്യൂരിറ്റി വിഭാഗത്തെയും, CERT-നെയും (Computer Emergency Response Team, Kerala) അറിയിക്കുകയും ആരോഗ്യ വകുപ്പ് മന്ത്രിയുടെ നിർദ്ദേശപ്രകാരം ചേർന്ന വിദഗ്ധ സമിതിയുടെ ചർച്ചയുടെ അടിസ്ഥാനത്തിൽ സത്വര നടപടികൾ സ്വീകരിക്കുകയും ചെയ്തു. ആർസി സി യിൽ നിന്നും 29/04/2024-ന് ഔദ്യോഗികമായി Superintendent of Police, Cyber Operations ന് പരാതി നൽകിയപ്പോൾ ലഭ്യമായ നിർദേശപ്രകാരം, 08/05/2024 ന് തിരുവനന്തപുരം പോലീസ് കമ്മീഷണർക്ക് പരാതി സമർപ്പിക്കുകയും ആയതിന്റെ അടിസ്ഥാനത്തിൽ 09/05/2024-ന് സൈബർ ക്രൈം വിഭാഗം 0116/2024 നമ്പറായി FIR രജിസ്റ്റർ ചെയ്യുകയും ചെയ്തു. ഇതിനെ തുടർന്ന് ഇൻഫെക്ടഡ് ആയ 12 കംപ്യൂട്ടറുകളിലുള്ള വിവരങ്ങൾ പുനഃസ്ഥാപിക്കുന്നതിനു വേണ്ടി 5 ദിവസം സ്ഥാപനത്തിലെ രോഗികളുടെ

			ചികിത്സ നിർത്തി വയ്ക്കുകയും ആറാം ദിനം പുനരാരംഭിക്കുകയും ചെയ്തു. സൈബർ ആക്രമണം നേരിട്ട മറ്റ് കംപ്യൂട്ടറുകൾ സൈബർ വിഭാഗം തുടർപരിശോധനകൾക്ക് വേണ്ടി എടുത്തിട്ടുണ്ട്. കൂടാതെ സൈബർ വിഭാഗത്തിന്റെയും സെർട്ടിന്റെയും നിർദ്ദേശപ്രകാരം രോഗികളുടെ ചികിത്സാ രേഖകൾക്ക് കൂടുതൽ സുരക്ഷ ഉറപ്പാക്കുന്നതിനും ഭാവിയിൽ ഇത്തരം സൈബർ അറ്റാക്കുകൾ വരാതിരിക്കുന്നതിനുമുള്ള നടപടികൾ RCC സ്വീകരിച്ചു വരികയാണ്. എന്നാൽ ബാക്കപ്പ് ഉള്ളതിനാൽ രോഗികളുടെ റേഡിയേഷൻ ചികിത്സാ വിവരങ്ങൾ സുരക്ഷിതമാണ്.
(ബി)	സൈബർ ആക്രമണത്തിന്റെ ഫലമായി രോഗികളുടെ ആരോഗ്യവിവരങ്ങൾ ചോർന്നിരുന്നോ എന്ന് പരിശോധിച്ചിട്ടുണ്ടോ; ഉണ്ടെങ്കിൽ പരിശോധനയിലെ കണ്ടെത്തലുകൾ എന്തെല്ലാമാണെന്നും ഏതെല്ലാം വിവരങ്ങളാണ് ചോർന്നിട്ടുള്ളതെന്നും വ്യക്തമാക്കാമോ?	(ബി)	RCC-യിലെ ransomware ആക്രമണത്തെക്കുറിച്ച് അന്വേഷണ ഏജൻസികളായ CERT ഉം സൈബർ വിഭാഗവും സമഗ്രമായ അന്വേഷണം നടത്തിവരികയാണ്. അന്വേഷണ റിപ്പോർട്ട് ലഭ്യമാകുന്ന മുറയ്ക്ക് തുടർ നടപടി സ്വീകരിക്കുന്നതാണ്.

സെക്ഷൻ ഓഫീസർ