**15 –ാം കേരള നിയമസഭ**

**11 –ാം സമ്മേളനം**

**നക്ഷത്രചിഹ്നമിട്ട ചോദ്യം നം. 457** **08-07-2024 - ൽ മറുപടിയ്ക്ക്**

**ആശുപത്രികളിലെ സോഫ്റ്റ്വെയറുകൾ ഹാക്ക് ചെയ്യുന്നത് തടയാൻ നടപടി**

| ചോദ്യം | | ഉത്തരം | |
|---|---|---|---|
| **ശ്രീ. സജീവ് ജോസഫ്,**<br>**ശ്രീ. എം. വിൻസെന്റ്,**<br>**ശ്രീ. ടി. ജെ. വിനോദ്** | | **ശ്രീമതി വീണാ ജോർജ്ജ്**<br>**(ആരോഗ്യ- വനിത-ശിശുവികസന വകുപ്പ് മന്ത്രി)** | |
| (എ) | സംസ്ഥാനത്തെ ആശുപത്രികളിലെ സോഫ്റ്റ്വെയറുകൾ ഹാക്ക് ചെയ്യുന്നത് തടയാൻ സ്വീകരിച്ച നടപടികൾ വിശദമാക്കുമോ; | (എ) | സംസ്ഥാനത്തെ അലോപ്പതി ആശുപത്രികളിൽ നിലവിൽ നടപ്പിലാക്കിയിട്ടുള്ളതും നടപ്പിലാക്കി വരുന്നതുമായ ഒരു കേന്ദ്രീകൃത സോഫ്റ്റ് വെയറാണ് ഇ-ഹെൽത്ത് ഹോസ്പിറ്റൽ മാനേജ്മെന്റ് സിസ്റ്റം (എച്ച്എംഎസ്). ഈ സോഫ്റ്റ്വെയർ നിലവിൽ സ്റ്റേറ്റ് ഡാറ്റ സെന്ററിലാണ് സ്ഥാപിച്ചിട്ടുള്ളത്. സംസ്ഥാന സർക്കാരിന്റെ സ്റ്റേറ്റ് ഡാറ്റ സെന്ററിൽ ലഭ്യമായിട്ടുള്ള എല്ലാ സാങ്കേതിക സുരക്ഷാ സംവിധാനങ്ങളും ഇ-ഹെൽത്ത് സോഫ്റ്റ്വെയർ പ്രയോജനപ്പെടുത്തുന്നുണ്ട്. ഇവയിൽ ഫയർവാൾ സംരക്ഷണം, SIEM (സെക്യൂരിറ്റി ഇൻഫർമേഷൻ ആൻഡ് ഇവന്റ് മാനേജ്മെന്റ്) മുതലായവ ഉൾപ്പെടുന്ന സ്റ്റേറ്റ് ഡാറ്റ സെന്റർ (SDC) നടപ്പിലാക്കിയ എല്ലാ സുരക്ഷാ സംവിധാനങ്ങളുമുണ്ട്. കൂടാതെ പ്രത്യേക സുരക്ഷ ഉറപ്പാക്കുന്നതിലേക്കായി ഇ-ഹെൽത്ത് നേരിട്ട് വെബ് ആപ്ലിക്കേഷൻ ഫയർവാൾ നടപ്പിലാക്കിയിട്ടുമുണ്ട്. സുരക്ഷ ശക്തമാക്കുന്നതിന്റെ ഭാഗമായി HTTPS (ഹൈപ്പർടെക്സ്റ്റ് ട്രാൻസ്ഫർ പ്രോട്ടോക്കോൾ സെക്യൂർ) പ്രോട്ടോക്കോൾ ഉറപ്പാക്കിയിട്ടുണ്ട്. KSWAN/KFON/MPLS/VPN എന്നീ സർക്കാർ നെറ്റ്-വർക്കുകൾ വഴി മാത്രമേ ആപ്ലിക്കേഷനിലേക്കുള്ള പ്രവേശനം സാധ്യമാകൂ. ഇന്റർനെറ്റിലേക്കുള്ള ആക്സസ് പരിമിതപ്പെടുത്തുന്നതിലൂടെയും ആപ്ലിക്കേഷൻ ആക്സസ് ചെയ്യുന്നതിനായി നടപ്പിലാക്കിയ സിംഗിൾ-സൈൻ-ഓൺ-മെക്കാനിസം വഴിയും, ഹോസ്പിറ്റൽ നെറ്റ്വർക്കിൽ നിന്ന് ആധികാരിക ഉപയോക്താക്കൾക്ക് മാത്രമേ ആപ്ലിക്കേഷൻ ആക്സസ് ചെയ്യാനാകൂ എന്നും ഉറപ്പാക്കുന്നു. കൂടാതെ, ഇ-ഹെൽത്ത് വികസിപ്പിച്ച എല്ലാ ആപ്ലിക്കേഷനുകളും സെക്യൂരിറ്റി ഓഡിറ്റ് പ്രക്രിയ പൂർത്തിയാക്കിയതിന് ശേഷം മാത്രമേ സ്റ്റേറ്റ് ഡാറ്റാ |

| | | | |
|---|---|---|---|
| | | | സെന്ററിൽ ഹോസ്റ്റ് ചെയ്യപ്പെടുകയുള്ളൂ. മാത്രവുമല്ല ഹോസ്റ്റ് ചെയ്തതിന് ശേഷം ഇൻകമിംഗ്/ ഔട്ട്ഗോയിംഗ് വെബ് ട്രാഫിക് പതിവായി നിരീക്ഷിക്കുകയും ചെയ്യുന്നു. |
| (ബി) | തിരുവനന്തപുരത്തെ റീജിയണൽ ക്യാൻസർ സെന്ററിൽ റേഡിയേഷൻ ചികിത്സയ്ക്കുള്ള സോഫ്റ്റ്വെയറിലടക്കം വിദേശ സൈബർ ആക്രമണം നടന്നതായി പറയുന്നത് ഗൗരവത്തോടെ കാണുന്നുണ്ടോ; | (ബി) | റേഡിയോ ഡയഗ്നോസിസ് വിഭാഗത്തിലെ M/s GE കമ്പനിയുടെ PACS സോഫ്റ്റ്വെയറിലും റേഡിയേഷൻ ഫിസിക്സ് വിഭാഗത്തിലെ M/s VARIAN കമ്പനിയുടെ CITRIX സോഫ്റ്റ്വെയറിലും ആണ് ആക്രമണം നേരിട്ടത്. സൈബർ ആക്രമണം കണ്ടെത്തിയതിന്റെ ആദ്യ ദിനം മുതൽ തന്നെ അതിനെ മറ്റ് കംപ്യൂട്ടറുകളിൽ വ്യാപിക്കാതിരിക്കാനുള്ള നടപടികൾ RCC സ്വീകരിച്ചിരുന്നു. അടിയന്തിരമായി സർക്കാരിനെയും സൈബർ സെക്യൂരിറ്റി വിഭാഗത്തെയും സെർട്ടിനെയും (Computer Emergency Response Team, Kerala) അറിയിക്കുകയും ആരോഗ്യ വകുപ്പ് മന്ത്രിയുടെ നേതൃത്വത്തിൽ നടത്തിയ ചർച്ചയുടെ അടിസ്ഥാനത്തിൽ സത്വര നടപടികൾ സ്വീകരിക്കുകയും ചെയ്തു. സൈബർ വിഭാഗവും സെർട്ടും അനാലിസിസ് നടത്തിയതിന്റെ അടിസ്ഥാനത്തിൽ 7 ഡെസ്ക്ടോപ്പ് പിസികളിലും 4 സെർവറുകളിലും ആണ് വൈറസ് ബാധിച്ചതെന്നും കണ്ടുപിടിച്ചു. തുടർന്ന് ഇൻഫെക്ടഡ് ആയിട്ടുള്ള കംപ്യൂട്ടറുകളിൽ ഉള്ള വിവരങ്ങൾ പുനഃസ്ഥാപിക്കുന്നതിനു വേണ്ടി 5 ദിവസം ചികിത്സ നിർത്തി വയ്ക്കുകയും ആറാം ദിനം പുനരാരംഭിക്കുകയും ചെയ്തു. സൈബർ ആക്രമണം നേരിട്ട മറ്റ് കംപ്യൂട്ടറുകൾ സൈബർ വിഭാഗം തുടർ പരിശോധനകൾക്ക് വേണ്ടി എടുത്തിട്ടുണ്ട്. സൈബർ വിഭാഗത്തിന്റെയും സെർട്ടിന്റെയും നിർദ്ദേശപ്രകാരം രോഗികളുടെ ചികിത്സാരേഖകൾക്ക് കൂടുതൽ സുരക്ഷ ഉറപ്പാക്കുന്നതിനും ഭാവിയിൽ ഇത്തരം സൈബർ ആക്രമണങ്ങൾ വരാതിരിക്കുന്നതിനും ഉള്ള നടപടികൾ RCC സ്വീകരിച്ചു വരികയാണ്. ബാക്കപ്പ് ഉള്ളതിനാൽ രോഗികളുടെ റേഡിയേഷൻ ചികിത്സാവിവരങ്ങൾ സുരക്ഷിതമാണ്. |
| (സി) | എങ്കിൽ ഇക്കാര്യത്തിൽ സ്വീകരിച്ച നടപടികൾ എന്തൊക്കെയാണെന്ന് വ്യക്തമാക്കുമോ? | (സി) | റേഡിയോ ഡയഗ്നോസിസ് വിഭാഗത്തിലെ M/s GE കമ്പനിയുടെ PACS സോഫ്റ്റ്വെയറിലും റേഡിയേഷൻ ഫിസിക്സ് വിഭാഗത്തിലെ M/s VARIAN കമ്പനിയുടെ CITRIX സോഫ്റ്റ്വെയറിലും ആണ് ആക്രമണം നേരിട്ടത്. സൈബർ ആക്രമണം കണ്ടെത്തിയതിന്റെ ആദ്യ ദിനം മുതൽ തന്നെ അതിനെ മറ്റ് കംപ്യൂട്ടറുകളിൽ വ്യാപിക്കാതിരിക്കാനുള്ള നടപടികൾ RCC സ്വീകരിച്ചിരുന്നു. അടിയന്തിരമായി സർക്കാരിനെയും സൈബർ സെക്യൂരിറ്റി |

| | | | |
|---|---|---|---|
| | | | വിഭാഗത്തെയും സെർട്ടിനെയും (Computer Emergency Response Team, Kerala) അറിയിക്കുകയും ആരോഗ്യ വകുപ്പ് മന്ത്രിയുടെ നേതൃത്വത്തിൽ നടത്തിയ ചർച്ചയുടെ അടിസ്ഥാനത്തിൽ സത്വര നടപടികൾ സ്വീകരിക്കുകയും ചെയ്തു. സൈബർ വിഭാഗവും സെർട്ടും അനാലിസിസ് നടത്തിയതിന്റെ അടിസ്ഥാനത്തിൽ 7 ഡെസ്ക്ടോപ്പ് പിസികളിലും 4 സെർവറുകളിലും ആണ് വൈറസ് ബാധിച്ചതെന്നും കണ്ടുപിടിച്ചു. തുടർന്ന് ഇൻഫെക്ടഡ് ആയിട്ടുള്ള കംപ്യൂട്ടറുകളിൽ ഉള്ള വിവരങ്ങൾ പുനഃസ്ഥാപിക്കുന്നതിനു വേണ്ടി 5 ദിവസം ചികിത്സ നിർത്തി വയ്ക്കുകയും ആറാം ദിനം പുനരാരംഭിക്കുകയും ചെയ്തു. സൈബർ ആക്രമണം നേരിട്ട മറ്റു കംപ്യൂട്ടറുകൾ സൈബർ വിഭാഗം തുടർ പരിശോധനകൾക്ക് വേണ്ടി എടുത്തിട്ടുണ്ട്. സൈബർ വിഭാഗത്തിന്റെയും സെർട്ടിന്റെയും നിർദ്ദേശപ്രകാരം രോഗികളുടെ ചികിത്സാരേഖകൾക്ക് കൂടുതൽ സുരക്ഷ ഉറപ്പാക്കുന്നതിനും ഭാവിയിൽ ഇത്തരം സൈബർ ആക്രമണങ്ങൾ വരാതിരിക്കുന്നതിനും ഉള്ള നടപടികൾ RCC സ്വീകരിച്ചു വരികയാണ്. ബാക്കപ്പ് ഉള്ളതിനാൽ രോഗികളുടെ റേഡിയേഷൻ ചികിത്സാവിവരങ്ങൾ സുരക്ഷിതമാണ്. |

സെക്ഷൻ ഓഫീസർ