ಡಿಜಿಟಲ್ ನಿರರ್ಗಳತೆ

4 ಕ್ಲೌಡ್ ಕಂಪ್ಯೂಟಿಂಗ್ ಮತ್ತು ಅದರ ಸೇವಾ ಮಾದರಿಗಳು

Q1. ಕ್ಲೌಡ್ ಕಂಪ್ಯೂಟಿಂಗ್ ಎಂದರೇನು?

- ಕ್ಲೌಡ್ ಕಂಪ್ಯೂಟಿಂಗ್ ಎನ್ನುವುದು ಡೇಟಾವನ್ನು ಸಂಗ್ರಹಿಸಲು, ನಿರ್ವಹಿಸಲು ಮತ್ತು ಪ್ರಕ್ರಿಯೆಗೊಳಿಸಲು ಇಂಟರ್ನೆಟ್ ಮೂಲಕ ಹೋಸ್ಟ್ ಮಾಡಲಾದ ರಿಮೋಟ್ ಸರ್ವರ್‌ಗಳ ನೆಟ್‌ವರ್ಕ್ ಅನ್ನು ಬಳಸುವ ಪ್ರಕ್ರಿಯೆಯಾಗಿದೆ.
- ಕ್ಲೌಡ್ ಕಂಪ್ಯೂಟಿಂಗ್ ಎನ್ನುವುದು ಸ್ಥಳೀಯ ಸರ್ವರ್ ಅಥವಾ ಪರ್ಸನಲ್ ಕಂಪ್ಯೂಟರ್‌ಗಿಂತ ಹೆಚ್ಚಾಗಿ ಇಂಟರ್ನೆಟ್‌ನಿಂದ ಡೇಟಾವನ್ನು ಸಂಗ್ರಹಿಸುವ, ನಿರ್ವಹಿಸುವ ಮತ್ತು ಪ್ರವೇಶಿಸುವ ಪ್ರಕ್ರಿಯೆಯಾಗಿದೆ.
- ಕ್ಲೌಡ್ ಕಂಪ್ಯೂಟಿಂಗ್ ಎನ್ನುವುದು ಇಂಟರ್ನೆಟ್ ಮೂಲಕ ಕಂಪ್ಯೂಟಿಂಗ್ ಸೇವೆಗಳ ವಿತರಣೆಯಾಗಿದೆ

Q2. ಕ್ಲೌಡ್ ಕಂಪ್ಯೂಟಿಂಗ್ ಅನ್ನು ಬಳಸಿಕೊಂಡು ಯಾವ ಕಾರ್ಯಾಚರಣೆಗಳನ್ನು ನಿರ್ವಹಿಸಲಾಗುತ್ತದೆ?

- ಕ್ಲೌಡ್ ಕಂಪ್ಯೂಟಿಂಗ್ ಬಳಸಿ ಕೆಳಗಿನ ಕಾರ್ಯಾಚರಣೆಗಳನ್ನು ನಡೆಸಲಾಗುತ್ತದೆ :
  - ಹೊಸ ಅಪ್ಲಿಕೇಶನ್‌ಗಳು ಮತ್ತು ಸೇವೆಗಳನ್ನು ಅಭಿವೃದ್ಧಿಪಡಿಸುವುದು
  - ಡೇಟಾ ಸಂಗ್ರಹಣೆ, ಬ್ಯಾಕಪ್ ಮತ್ತು ಮರುಪಡೆಯುವಿಕೆ
  - ಬ್ಲಾಗ್‌ಗಳು ಮತ್ತು ವೆಬ್‌ಸೈಟ್‌ಗಳನ್ನು ಹೋಸ್ಟ್ ಮಾಡುವುದು
  - ಬೇಡಿಕೆಯ ಮೇರೆಗೆ ಸಾಫ್ಟ್‌ವೇರ್ ವಿತರಣೆ
  - ಡೇಟಾದ ವಿಶ್ಲೇಷಣೆ
  - ಸ್ಟ್ರೀಮಿಂಗ್ ವೀಡಿಯೊಗಳು ಮತ್ತು ಆಡಿಯೊಗಳು

Q3. ಕ್ಲೌಡ್ ಕಂಪ್ಯೂಟಿಂಗ್ ಏಕೆ?

- ಕ್ಲೌಡ್ ಕಂಪ್ಯೂಟಿಂಗ್ ತುಂಬಾ ಮುಖ್ಯವಾಗಿದೆ ಏಕೆಂದರೆ ಇದು ನಮ್ಯತೆ, ಡೇಟಾ ಮರುಪಡೆಯುವಿಕೆ, ಯಾವುದೇ ನಿರ್ವಹಣೆ, ಸುಲಭ ಪ್ರವೇಶ ಮತ್ತು ಉನ್ನತ ಮಟ್ಟದ ಸುರಕ್ಷತೆಯನ್ನು ನೀಡುತ್ತದೆ
- ಕ್ಲೌಡ್ ಕಂಪ್ಯೂಟಿಂಗ್ ಬಳಕೆಯಿಂದ ವ್ಯಾಪಾರ ಕಾರ್ಯಾಚರಣೆಗಳಲ್ಲಿ ದಕ್ಷತೆಯನ್ನು ಸಾಧಿಸಲಾಗುತ್ತದೆ
- ಕ್ಲೌಡ್ ಕಂಪ್ಯೂಟಿಂಗ್ ದೊಡ್ಡ ಡೇಟಾ, ಸೈಬರ್-ಸುರಕ್ಷತೆ ಮತ್ತು ಗುಣಮಟ್ಟದ ನಿಯಂತ್ರಣವನ್ನು ನಿರ್ವಹಿಸಲು ಸಹಾಯ ಮಾಡುತ್ತದೆ
- ಕ್ಲೌಡ್ ಕಂಪ್ಯೂಟಿಂಗ್ ಸಂಸ್ಥೆಗಳು ತಮ್ಮ ಉತ್ಪನ್ನಗಳು ಮತ್ತು ಸೇವೆಗಳನ್ನು ಮೊದಲಿಗಿಂತ ಉತ್ತಮ ರೀತಿಯಲ್ಲಿ ತಲುಪಿಸಲು ಸಹಾಯ ಮಾಡಿದೆ

Q4. ಮೋಡ ಎಂದರೇನು?

- ಮೋಡವು ಇಂಟರ್ನೆಟ್ ಆಗಿದೆ

Q5. ಕ್ಲೌಡ್ ಕಂಪ್ಯೂಟಿಂಗ್‌ನ ಪ್ರಯೋಜನಗಳೇನು?

ಕ್ಲೌಡ್ ಕಂಪ್ಯೂಟಿಂಗ್‌ನ ಪ್ರಯೋಜನಗಳೆಂದರೆ:

1. ಬ್ಯಾಕ್-ಅಪ್ ಮತ್ತು ಡೇಟಾ ಮರುಸ್ಥಾಪನೆ 2. ಸುಧಾರಿತ ಸಹಯೋಗ 3. ಅತ್ಯುತ್ತಮ ಪ್ರವೇಶಸಾಧ್ಯತೆ

4. ಕಡಿಮೆ ನಿರ್ವಹಣಾ ವೆಚ್ಚ 5. ಮೊಬಿಲಿಟಿ 6. ಪೇ-ಪರ್-ಯೂಸ್ ಮಾದರಿಯಲ್ಲಿ ಸೇವೆಗಳು

7. ಅನಿಯಮಿತ ಸಂಗ್ರಹ ಸಾಮರ್ಥ್ಯ 8. ಡೇಟಾ ಭದ್ರತೆ

1.ಬ್ಯಾಕಪ್ ಮತ್ತು ಡೇಟಾವನ್ನು ಮರುಸ್ಥಾಪಿಸಿ

- ಡೇಟಾವನ್ನು ಕ್ಲೌಡ್‌ನಲ್ಲಿ ಸಂಗ್ರಹಿಸಿದ ನಂತರ, ಕ್ಲೌಡ್ ಅನ್ನು ಬಳಸಿಕೊಂಡು ಆ ಡೇಟಾವನ್ನು ಬ್ಯಾಕ್-ಅಪ್ ಪಡೆಯಲು ಮತ್ತು ಮರುಸ್ಥಾಪಿಸಲು ಸುಲಭವಾಗುತ್ತದೆ

2.ಸುಧಾರಿತ ಸಹಯೋಗ

- ಕ್ಲೌಡ್ ಅಪ್ಲಿಕೇಶನ್‌ಗಳು ಹಂಚಿದ ಸಂಗ್ರಹಣೆಯ ಮೂಲಕ ಕ್ಲೌಡ್‌ನಲ್ಲಿ ಮಾಹಿತಿಯನ್ನು ತ್ವರಿತವಾಗಿ ಮತ್ತು ಸುಲಭವಾಗಿ ಹಂಚಿಕೊಳ್ಳಲು ಜನರ ಗುಂಪುಗಳನ್ನು ಅನುಮತಿಸುವ ಮೂಲಕ ಸಹಯೋಗವನ್ನು ಸುಧಾರಿಸುತ್ತದೆ.

3.ಅತ್ಯುತ್ತಮ ಪ್ರವೇಶಸಾಧ್ಯತೆ

- ಇಂಟರ್ನೆಟ್ ಸಂಪರ್ಕವನ್ನು ಬಳಸಿಕೊಂಡು ಯಾವುದೇ ಸಮಯದಲ್ಲಿ, ಇಡೀ ಪ್ರಪಂಚದಲ್ಲಿ ಎಲ್ಲಿಯಾದರೂ ಮಾಹಿತಿಯನ್ನು ತ್ವರಿತವಾಗಿ ಮತ್ತು ಸುಲಭವಾಗಿ ಸಂಗ್ರಹಿಸಲು ಮತ್ತು ಪ್ರವೇಶಿಸಲು ಕ್ಲೌಡ್ ನಮಗೆ ಅನುಮತಿಸುತ್ತದೆ

4. ಕಡಿಮೆ ನಿರ್ವಹಣಾ ವೆಚ್ಚ

- ಕ್ಲೌಡ್ ಕಂಪ್ಯೂಟಿಂಗ್ ಸಂಸ್ಥೆಗಳಿಗೆ ಹಾರ್ಡ್‌ವೇರ್ ಮತ್ತು ಸಾಫ್ಟ್‌ವೇರ್ ನಿರ್ವಹಣೆ ವೆಚ್ಚಗಳನ್ನು ಕಡಿಮೆ ಮಾಡುತ್ತದೆ .

5.ಮೊಬಿಲಿಟಿ

- ಕ್ಲೌಡ್ ಕಂಪ್ಯೂಟಿಂಗ್ ಯಾವುದೇ ಸಾಧನದ ಮೂಲಕ ಎಲ್ಲಾ ಕ್ಲೌಡ್ ಡೇಟಾವನ್ನು ಸುಲಭವಾಗಿ ಪ್ರವೇಶಿಸಲು ನಮಗೆ ಅನುಮತಿಸುತ್ತದೆ.

6.ಪೇ-ಪರ್-ಯೂಸ್ ಮಾದರಿಯಲ್ಲಿ ಸೇವೆಗಳು

- ಕ್ಲೌಡ್ ಕಂಪ್ಯೂಟಿಂಗ್ ಕ್ಲೌಡ್‌ನಲ್ಲಿನ ಪ್ರವೇಶ ಸೇವೆಗಳಿಗಾಗಿ ಬಳಕೆದಾರರಿಗೆ ಅಪ್ಲಿಕೇಶನ್ ಪ್ರೋಗ್ರಾಮಿಂಗ್ ಇಂಟರ್‌ಫೇಸ್‌ಗಳನ್ನು (API ಗಳು) ನೀಡುತ್ತದೆ ಮತ್ತು ಸೇವೆಯ ಬಳಕೆಯ ಪ್ರಕಾರ ಶುಲ್ಕವನ್ನು ಪಾವತಿಸುತ್ತದೆ

7.ಅನಿಯಮಿತ ಸಂಗ್ರಹ ಸಾಮರ್ಥ್ಯ

- ಡಾಕ್ಯುಮೆಂಟ್‌ಗಳು, ಚಿತ್ರಗಳು, ಆಡಿಯೋ, ವೀಡಿಯೋ ಮುಂತಾದ ಪ್ರಮುಖ ಡೇಟಾವನ್ನು ಒಂದೇ ಸ್ಥಳದಲ್ಲಿ ಸಂಗ್ರಹಿಸಲು ಕ್ಲೌಡ್ ದೊಡ್ಡ ಪ್ರಮಾಣದ ಶೇಖರಣಾ ಸಾಮರ್ಥ್ಯವನ್ನು ನೀಡುತ್ತದೆ

8.ಡೇಟಾ ಸೆಕ್ಯುರಿಟಿ

- ಕ್ಲೌಡ್ ಭದ್ರತೆಗೆ ಸಂಬಂಧಿಸಿದ ಹಲವು ಸುಧಾರಿತ ವೈಶಿಷ್ಟ್ಯಗಳನ್ನು ನೀಡುತ್ತದೆ ಮತ್ತು ಡೇಟಾವನ್ನು ಸುರಕ್ಷಿತವಾಗಿ ಸಂಗ್ರಹಿಸಲಾಗಿದೆ ಮತ್ತು ನಿರ್ವಹಿಸಲಾಗಿದೆ ಎಂದು ಖಚಿತಪಡಿಸುತ್ತದೆ

Q6. ಕ್ಲೌಡ್ ಸೇವಾ ಮಾದರಿಗಳು ಯಾವುವು?

- ಕ್ಲೌಡ್ ಸೇವಾ ಮಾದರಿಗಳಲ್ಲಿ ಮೂರು ವಿಧಗಳಿವೆ. ಅವು ಈ ಕೆಳಗಿನಂತಿವೆ:-

1. ಮೂಲಸೌಕರ್ಯ ಸೇವೆಯಾಗಿ (IaaS)
2. ಒಂದು ಸೇವೆಯಾಗಿ ವೇದಿಕೆ (PaaS)
3. ಸೇವೆಯಾಗಿ ಸಾಫ್ಟ್‌ವೇರ್ (SaaS)

Q7. ಕ್ಲೌಡ್ ಸೇವೆಗಳ ಟಿ ವೈಗಳನ್ನು ವಿವರಿಸಿ

ಕ್ಲೌಡ್ ಸೇವೆಗಳ ವಿಧಗಳು:

1. ಮೂಲಸೌಕರ್ಯ ಸೇವೆಯಾಗಿ (IaaS)
2. ಒಂದು ಸೇವೆಯಾಗಿ ವೇದಿಕೆ (PaaS)
3. ಸೇವೆಯಾಗಿ ಸಾಫ್ಟ್‌ವೇರ್ (SaaS)

1. ಸೇವೆಯಾಗಿ ಮೂಲಸೌಕರ್ಯ (IaaS)

- IaaS ಕ್ಲೌಡ್ ಕಂಪ್ಯೂಟಿಂಗ್ ಸೇವೆಗಳ ಅತ್ಯಂತ ಮೂಲಭೂತ ವರ್ಗವಾಗಿದೆ
- IaaS ನೊಂದಿಗೆ, ಕ್ಲೌಡ್ ಪ್ರೊವೈಡರ್‌ನಿಂದ ಪಾವತಿಸಿದ ಆಧಾರದ ಮೇಲೆ ನೀವು ಐಟಿ ಮೂಲಸೌಕರ್ಯ-ಸರ್ವರ್‌ಗಳು ಮತ್ತು ವರ್ಚುವಲ್ ಯಂತ್ರಗಳು (ವಿಎಂಗಳು), ಸಂಗ್ರಹಣೆ, ನೆಟ್‌ವರ್ಕ್‌ಗಳು, ಆಪರೇಟಿಂಗ್ ಸಿಸ್ಟಮ್‌ಗಳನ್ನು ಬಾಡಿಗೆಗೆ ಪಡೆಯುತ್ತೀರಿ.

2. ಒಂದು ಸೇವೆಯಾಗಿ ವೇದಿಕೆ (PaaS)

- PaaS ಸಾಫ್ಟ್‌ವೇರ್ ಅಪ್ಲಿಕೇಶನ್‌ಗಳನ್ನು ಅಭಿವೃದ್ಧಿಪಡಿಸಲು, ಪರೀಕ್ಷಿಸಲು, ವಿತರಿಸಲು ಮತ್ತು ನಿರ್ವಹಿಸಲು ಬೇಡಿಕೆಯ ಪರಿಸರವನ್ನು ಒದಗಿಸುವ ಕ್ಲೌಡ್ ಕಂಪ್ಯೂಟಿಂಗ್ ಸೇವೆಗಳನ್ನು ಸೂಚಿಸುತ್ತದೆ.
- ಡೆವಲಪರ್‌ಗಳಿಗೆ ವೆಬ್ ಅಥವಾ ಮೊಬೈಲ್ ಅಪ್ಲಿಕೇಶನ್‌ಗಳನ್ನು ತ್ವರಿತವಾಗಿ ರಚಿಸಲು ಸುಲಭವಾಗುವಂತೆ PaaS ಅನ್ನು ವಿನ್ಯಾಸಗೊಳಿಸಲಾಗಿದೆ, ಸರ್ವರ್‌ಗಳು, ಸಂಗ್ರಹಣೆ, ನೆಟ್‌ವರ್ಕ್ ಮತ್ತು ಅಭಿವೃದ್ಧಿಗೆ ಅಗತ್ಯವಿರುವ ಡೇಟಾಬೇಸ್‌ಗಳ ಆಧಾರವಾಗಿರುವ ಮೂಲಸೌಕರ್ಯವನ್ನು ಹೊಂದಿಸುವ ಅಥವಾ ನಿರ್ವಹಿಸುವ ಬಗ್ಗೆ ಚಿಂತಿಸದೆ

3. ಸೇವೆಯಾಗಿ ಸಾಫ್ಟ್‌ವೇರ್ (SaaS)

- SaaS ಎನ್ನುವುದು ಸಾಫ್ಟ್‌ವೇರ್ ಅಪ್ಲಿಕೇಶನ್‌ಗಳನ್ನು ಇಂಟರ್ನೆಟ್‌ನಲ್ಲಿ, ಬೇಡಿಕೆಯ ಮೇರೆಗೆ ಮತ್ತು ಸಾಮಾನ್ಯವಾಗಿ ಚಂದಾದಾರಿಕೆಯ ಆಧಾರದ ಮೇಲೆ ತಲುಪಿಸುವ ಒಂದು ವಿಧಾನವಾಗಿದೆ
- SaaS ನೊಂದಿಗೆ, ಕ್ಲೌಡ್ ಪೂರೈಕೆದಾರರು ಸಾಫ್ಟ್‌ವೇರ್ ಅಪ್ಲಿಕೇಶನ್ ಮತ್ತು ಆಧಾರವಾಗಿರುವ ಮೂಲಸೌಕರ್ಯವನ್ನು ಹೋಸ್ಟ್ ಮಾಡಿ ಮತ್ತು ನಿರ್ವಹಿಸುತ್ತಾರೆ ಮತ್ತು ಸಾಫ್ಟ್‌ವೇರ್ ನವೀಕರಣಗಳು ಮತ್ತು ಭದ್ರತಾ ಪ್ಯಾಚಿಂಗ್‌ನಂತಹ ಯಾವುದೇ ನಿರ್ವಹಣೆಯನ್ನು ನಿರ್ವಹಿಸುತ್ತಾರೆ
- ಬಳಕೆದಾರರು ತಮ್ಮ ಫೋನ್, ಟ್ಯಾಬ್ಲೆಟ್ ಅಥವಾ PC ಯಲ್ಲಿ ಸಾಮಾನ್ಯವಾಗಿ ವೆಬ್ ಬ್ರೌಸರ್ ನೊಂದಿಗೆ ಇಂಟರ್ನೆಟ್ ಮೂಲಕ ಅಪ್ಲಿಕೇಶನ್‌ಗೆ ಸಂಪರ್ಕ ಸಾಧಿಸುತ್ತಾರೆ

Q 6. IaaS, PaaS ಮತ್ತು SaaS ನಡುವೆ ವ್ಯತ್ಯಾಸವನ್ನು ಗುರುತಿಸಿ

IaaS	Paas	SaaS
It provides a virtual data center to store information and create platforms for app development, testing, and deployment.	It provides virtual platforms and tools to create, test, and deploy apps.	It provides web software and apps to complete business tasks.
It provides access to resources such as virtual machines, virtual storage, etc.	It provides runtime environments and deployment tools for applications.	It provides software as a service to the end-users.
It is used by network architects.	It is used by developers.	It is used by end users.
IaaS provides only Infrastructure.	PaaS provides Infrastructure + Platform.	SaaS provides Infrastructure + Platform + Software.

Q7. ವಿವಿಧ ರೀತಿಯ ಮೇಘಗಳನ್ನು ವಿವರಿಸಿ

ಮೇಘದ ವಿಧಗಳೆಂದರೆ:

1. ಸಾರ್ವಜನಿಕ ಮೇಘ
2. ಖಾಸಗಿ ಮೇಘ
3. ಹೈಬ್ರಿಡ್ ಕ್ಲೌಡ್4. ಸಮುದಾಯ ಮೇಘ

1. ಸಾರ್ವಜನಿಕ ಮೇಘ

- ಪೇ-ಪರ್-ಯೂಸೇಜ್ ಅನ್ನು ಬಳಸಿಕೊಂಡು ಇಂಟರ್ನೆಟ್ ಮೂಲಕ ಮಾಹಿತಿಯನ್ನು ಸಂಗ್ರಹಿಸಲು ಮತ್ತು ಪ್ರವೇಶಿಸಲು ಸಾರ್ವಜನಿಕ ಕ್ಲೌಡ್ ಎಲ್ಲರಿಗೂ ತೆರೆದಿರುತ್ತದೆ ವಿಧಾನ
- ಸಾರ್ವಜನಿಕ ಕ್ಲೌಡ್ ಎನ್ನುವುದು ಮುಕ್ತ ವ್ಯವಸ್ಥೆಯಾಗಿದ್ದು, ಅಲ್ಲಿ ಸಂಗ್ರಹಣೆ ಅಥವಾ ಸಾಫ್ಟ್‌ವೇರ್ ಉಚಿತವಾಗಿ ಲಭ್ಯವಿದೆ ಅಥವಾ ಇಂಟರ್ನೆಟ್ ಮೂಲಕ ಪ್ರವೇಶಿಸಬಹುದಾದ ಪ್ರತಿ ಬಳಕೆಯ ಮಾದರಿಗೆ ಪಾವತಿಸಿ
- ಸಾರ್ವಜನಿಕ ಕ್ಲೌಡ್‌ನಲ್ಲಿ, ಕಂಪ್ಯೂಟಿಂಗ್ ಸಂಪನ್ಮೂಲಗಳನ್ನು ಕ್ಲೌಡ್ ಸೇವಾ ಪೂರೈಕೆದಾರರಿಂದ ನಿರ್ವಹಿಸಲಾಗುತ್ತದೆ ಮತ್ತು ನಿರ್ವಹಿಸಲಾಗುತ್ತದೆ (CSP)
- **ಉದಾಹರಣೆ:** Amazon elastic compute cloud (EC2), IBM Smart Cloud Enterprise, Microsoft-Google App ಎಂಜಿನ್, ವಿಂಡೋಸ್ ಅಜುರೆ ಸೇವೆಗಳ ವೇದಿಕೆ

2. ಖಾಸಗಿ ಮೇಘ

- ಪಿ ರಿವೇಟ್ ಕ್ಲೌಡ್ ಅನ್ನು ಆಂತರಿಕ ಕ್ಲೌಡ್ ಅಥವಾ ಕಾರ್ಪೊರೇಟ್ ಕ್ಲೌಡ್ ಎಂದೂ ಕರೆಯಲಾಗುತ್ತದೆ
- ಖಾಸಗಿ ಕ್ಲೌಡ್ ಫೈರ್‌ವಾಲ್‌ಗಳು ಮತ್ತು ಆಂತರಿಕ ಹೋಸ್ಟಿಂಗ್ ಮೂಲಕ ಡೇಟಾಗೆ ಉನ್ನತ ಮಟ್ಟದ ಭದ್ರತೆ ಮತ್ತು ಗೌಪ್ಯತೆಯನ್ನು ಒದಗಿಸುತ್ತದೆ
- ಕಾರ್ಯಾಚರಣೆಯ ಮತ್ತು ಸೂಕ್ಷ್ಮ ಡೇಟಾವನ್ನು ಮೂರನೇ ವ್ಯಕ್ತಿಯ ಪೂರೈಕೆದಾರರಿಗೆ ಪ್ರವೇಶಿಸಲಾಗುವುದಿಲ್ಲ ಎಂದು ಇದು ಖಚಿತಪಡಿಸುತ್ತದೆ
- ಇದನ್ನು ನಿರ್ಮಿಸಲು ಸಂಸ್ಥೆಗಳು ಬಳಸುತ್ತವೆ ಮತ್ತು ತಮ್ಮ ಸ್ವಂತ ಡೇಟಾ ಕೇಂದ್ರಗಳನ್ನು ಆಂತರಿಕವಾಗಿ ಅಥವಾ ಮೂರನೇ ವ್ಯಕ್ತಿಯಿಂದ ನಿರ್ವಹಿಸಿ
- ಇದನ್ನು ಓಪನ್ ಸೋರ್ಸ್ ಉಪಕರಣಗಳನ್ನು ಬಳಸಿಕೊಂಡು ನಿಯೋಜಿಸಬಹುದು ಉದಾಹರಣೆಗೆ ಓಪನ್‌ಸ್ಟಾಕ್ ಮತ್ತು ಯೂಕಲಿಪ್ಟಸ್
- **ಉದಾಹರಣೆ:** HP ಡೇಟಾ ಕೇಂದ್ರಗಳು, ಮೈಕ್ರೋಸಾಫ್ಟ್, ಎಲಾಸ್ಟ್ರಾ-ಖಾಸಗಿ ಕ್ಲೌಡ್ ಮತ್ತು ಉಬುಂಟು ಖಾಸಗಿ ಮೋಡದ ಉದಾಹರಣೆ

3. ಹೈಬ್ರಿಡ್ ಮೇಘ

- ಹೈಬ್ರಿಡ್ ಕ್ಲೌಡ್ ಸಾರ್ವಜನಿಕ ಮೋಡ ಮತ್ತು ಖಾಸಗಿ ಮೋಡದ ಸಂಯೋಜನೆಯಾಗಿದೆ
- ಹೈಬ್ರಿಡ್ ಕ್ಲೌಡ್ ಭಾಗಶಃ ಸುರಕ್ಷಿತವಾಗಿದೆ ಏಕೆಂದರೆ ಸಾರ್ವಜನಿಕರ ಮೇಲೆ ಕಾರ್ಯನಿರ್ವಹಿಸುವ ಸೇವೆಗಳು ಕ್ಲೌಡ್ ಅನ್ನು ಯಾರಾದರೂ ಪ್ರವೇಶಿಸಬಹುದು, ಆದರೆ ಖಾಸಗಿ ಕ್ಲೌಡ್‌ನಲ್ಲಿ ಚಾಲನೆಯಲ್ಲಿರುವ ಸೇವೆಗಳನ್ನು ಪ್ರವೇಶಿಸಬಹುದು ಸಂಸ್ಥೆಯ ಬಳಕೆದಾರರಿಂದ ಮಾತ್ರ
- **ಉದಾಹರಣೆ:** Google Application Suite (Gmail, Google Apps, ಮತ್ತು Google Drive), Office 365 (ವೆಬ್‌ನಲ್ಲಿ MS ಆಫೀಸ್ ಮತ್ತು ಒಂದು ಡ್ರೈವ್), Amazon ವೆಬ್ ಸೇವೆಗಳು

4. ಸಮುದಾಯ ಮೇಘ

- ಸಮುದಾಯ ಕ್ಲೌಡ್ ಸಂಸ್ಥೆ ಮತ್ತು ನಿರ್ದಿಷ್ಟ ಸಮುದಾಯದ ನಡುವೆ ಮಾಹಿತಿಯನ್ನು ಹಂಚಿಕೊಳ್ಳಲು ಹಲವಾರು ಸಂಸ್ಥೆಗಳ ಗುಂಪಿನ ಮೂಲಕ ವ್ಯವಸ್ಥೆಗಳು ಮತ್ತು ಸೇವೆಗಳನ್ನು ಪ್ರವೇಶಿಸಲು ಅನುಮತಿಸುತ್ತದೆ
- ಇದು ಸಮುದಾಯದಲ್ಲಿ ಒಂದು ಅಥವಾ ಹೆಚ್ಚಿನ ಸಂಸ್ಥೆಗಳು, ಮೂರನೇ ವ್ಯಕ್ತಿ ಅಥವಾ ಅವುಗಳ ಸಂಯೋಜನೆಯಿಂದ ಒಡೆತನದಲ್ಲಿದೆ, ನಿರ್ವಹಿಸಲ್ಪಡುತ್ತದೆ ಮತ್ತು ನಿರ್ವಹಿಸುತ್ತದೆ
- **ಉದಾಹರಣೆ:** ಹೆಲ್ತ್ ಕೇರ್ ಸಮುದಾಯ ಕ್ಲೌಡ್

Q8. ಸಾರ್ವಜನಿಕ ಮೋಡ, ಖಾಸಗಿ ಮೋಡ, ಹೈಬ್ರಿಡ್ ಕ್ಲೌಡ್ ಮತ್ತು ಸಮುದಾಯ ಮೋಡದ ನಡುವೆ ವ್ಯತ್ಯಾಸವನ್ನು ಗುರುತಿಸಿ

Parameter	Public Cloud	Private Cloud	Hybrid Cloud	Community Cloud
Host	Service provider	Enterprise (Third party)	Enterprise (Third party)	Community (Third party)
Users	General public	Selected users	Selected users	Community members
Access	Internet	Internet, VPN	Internet, VPN	Internet, VPN
Owner	Service provider	Enterprise	Enterprise	Community

ಡಿಜಿಟಲ್ ನಿರರ್ಗಳತೆ

5. ಸೈಬರ್ ಭದ್ರತೆ ಮತ್ತು ಸೈಬರ್ ದಾಳಿಯ ವಿಧಗಳು

Q1. ಸೈಬರ್ ಭದ್ರತೆ ಎಂದರೇನು?

- ಸೈಬರ್ ಭದ್ರತೆಯು ಕಂಪ್ಯೂಟರ್ ನೆಟ್‌ವರ್ಕ್ ಭದ್ರತೆಯ ವಿಶೇಷತೆಯನ್ನು ಸೂಚಿಸುತ್ತದೆ, ಇದು ತಂತ್ರಜ್ಞಾನಗಳು, ನೀತಿಗಳು ಮತ್ತು ಕಾರ್ಯವಿಧಾನಗಳನ್ನು ಒಳಗೊಂಡಿರುತ್ತದೆ ಅದು ನೆಟ್‌ವರ್ಕ್ ಮಾಡಿದ ಕಂಪ್ಯೂಟರ್ ಸಿಸ್ಟಮ್‌ಗಳನ್ನು ಅನಧಿಕೃತ ಬಳಕೆ ಅಥವಾ ಹಾನಿಯಿಂದ ರಕ್ಷಿಸುತ್ತದೆ.
- ಸೈಬರ್ ಭದ್ರತೆಯು ಎಲೆಕ್ಟ್ರಾನಿಕ್ ಡೇಟಾ ಮತ್ತು ಮಾಹಿತಿಯ ರಕ್ಷಣೆಯಾಗಿದೆ

Q2. ನಮಗೆ ಸೈಬರ್ ಭದ್ರತೆ ಏಕೆ ಬೇಕು?

- ಸೈಬರ್ ಭದ್ರತೆಯು ಮುಖ್ಯವಾಗಿದೆ ಏಕೆಂದರೆ ಇದು ಎಲ್ಲಾ ವರ್ಗಗಳ ಡೇಟಾವನ್ನು ಕಳ್ಳತನ ಮತ್ತು ಹಾನಿಯಿಂದ ರಕ್ಷಿಸುತ್ತದೆ
- ಸೈಬರ್ ದಾಳಿಯ ಅಪಾಯವನ್ನು ಕಡಿಮೆ ಮಾಡಲು ಮತ್ತು ಸಿಸ್ಟಮ್‌ಗಳು ಮತ್ತು ಡೇಟಾವನ್ನು ಸುರಕ್ಷಿತಗೊಳಿಸಲು, ಬಲವಾದ ಸೈಬರ್ ಭದ್ರತೆಯ ಅಗತ್ಯವಿದೆ
- ಸೈಬರ್ ಭದ್ರತೆ ಇದು ನಿಮ್ಮನ್ನು ಅಥವಾ ನಿಮ್ಮ ಕಂಪನಿಯನ್ನು ಸಂಭಾವ್ಯ ಸೈಬರ್ ಬೆದರಿಕೆಗಳಿಂದ ರಕ್ಷಿಸುವುದರಿಂದ ಇದು ಮುಖ್ಯವಾಗಿದೆ

Q3. ಸೈಬರ್ ಭದ್ರತೆಗೆ ಕ್ರಮಗಳೇನು?

- ಅಪಾಯ ನಿರ್ವಹಣೆಯ ಆಡಳಿತ
- ಸುರಕ್ಷಿತ ಸಂರಚನೆ
- ನೆಟ್‌ವರ್ಕ್ ಭದ್ರತೆ
- ಬಳಕೆದಾರರ ಸವಲತ್ತುಗಳನ್ನು ನಿರ್ವಹಿಸುವುದು
- ಬಳಕೆದಾರರ ಶಿಕ್ಷಣ ಮತ್ತು ಜಾಗೃತಿ
- ಘಟನೆ ನಿರ್ವಹಣೆ
- ಮಾಲ್ವೇರ್ ತಡೆಗಟ್ಟುವಿಕೆ
- ಉಸ್ತುವಾರಿ

Q4. ವಿವಿಧ ರೀತಿಯ ಸೈಬರ್ ಭದ್ರತೆಯನ್ನು ವಿವರಿಸಿ

ಸೈಬರ್ ಭದ್ರತೆಯ ವಿಧಗಳು:

1. ನಿರ್ಣಾಯಕ ಮೂಲಸೌಕರ್ಯ ಭದ್ರತೆ
2. ಅಪ್ಲಿಕೇಶನ್ ಭದ್ರತೆ
3. ನೆಟ್ವರ್ಕ್ ಭದ್ರತೆ
4. ಕ್ಲೌಡ್ ಭದ್ರತೆ 5. ಇಂಟರ್ನೆಟ್ ಆಫ್ ಥಿಂಗ್ಸ್ (IOT) ಭದ್ರತೆ

1. ನಿರ್ಣಾಯಕ ಮೂಲಸೌಕರ್ಯ ಭದ್ರತೆ

- ನಿರ್ಣಾಯಕ ಮೂಲಸೌಕರ್ಯ ಭದ್ರತೆಯು ಆಧುನಿಕ ಸಮಾಜಗಳು ಅವಲಂಬಿಸಿರುವ ಸೈಬರ್-ಭೌತಿಕ ವ್ಯವಸ್ಥೆಗಳನ್ನು ಒಳಗೊಂಡಿದೆ
- ನಿರ್ಣಾಯಕ ಮೂಲಸೌಕರ್ಯವನ್ನು ಹೊಂದಿರುವ ವ್ಯವಸ್ಥೆಗಳನ್ನು ಸುರಕ್ಷಿತವಾಗಿರಿಸಲು ಇದನ್ನು ನಿಯೋಜಿಸಲಾಗಿದೆ
- ನಿರ್ಣಾಯಕ ಮೂಲಸೌಕರ್ಯದ ಸಾಮಾನ್ಯ ಉದಾಹರಣೆಗಳು:
    1. ವಿದ್ಯುತ್ ಜಾಲ
    2. ನೀರಿನ ಶುದ್ಧೀಕರಣ
    3. ಸಂಚಾರಿ ದೀಪಗಳು
    4. ಶಾಪಿಂಗ್ ಕೇಂದ್ರಗಳು
    5. ಆಸ್ಪತ್ರೆಗಳು

2.ಅಪ್ಲಿಕೇಶನ್ ಭದ್ರತೆ

- ಇದು ಆಪ್-ಮಟ್ಟದಲ್ಲಿ ಸೂಕ್ಷ್ಮ ಮಾಹಿತಿಯನ್ನು ರಕ್ಷಿಸುವ ಪ್ರಕ್ರಿಯೆಯಾಗಿದೆ
- ಅಪ್ಲಿಕೇಶನ್‌ನ ಅಭಿವೃದ್ಧಿ ಹಂತದಲ್ಲಿ ಉದ್ಭವಿಸಬಹುದಾದ ಬಾಹ್ಯ ಬೆದರಿಕೆಗಳನ್ನು ನಿಭಾಯಿಸಲು ಅಪ್ಲಿಕೇಶನ್ ಸುರಕ್ಷತೆಯು ಸಾಫ್ಟ್‌ವೇರ್ ಮತ್ತು ಹಾರ್ಡ್‌ವೇರ್ ವಿಧಾನಗಳನ್ನು ಬಳಸುತ್ತದೆ
- ಅನಧಿಕೃತ ಪ್ರವೇಶವನ್ನು ತಡೆಯಲು ಸಹಾಯ ಮಾಡುವ ಅಪ್ಲಿಕೇಶನ್ ಭದ್ರತೆಯ ವಿಧಗಳು :
    1. ಆಂಟಿವೈರಸ್ ಕಾರ್ಯಕ್ರಮಗಳು
    2. ಫೈರ್ವಾಲ್ಗಳು
    3. ಎನ್ಕ್ರಿಪ್ಷನ್ ಪ್ರೋಗ್ರಾಂ

3.ನೆಟ್‌ವರ್ಕ್ ಭದ್ರತೆ

- ನೆಟ್‌ವರ್ಕ್ ಭದ್ರತೆಯು ನೆಟ್‌ವರ್ಕ್‌ನ ಒಳಗೆ ಮತ್ತು ಹೊರಗಿನ ದಾಳಿಯಿಂದ ಕಂಪ್ಯೂಟರ್ ನೆಟ್‌ವರ್ಕ್‌ನ ರಕ್ಷಣೆಯನ್ನು ಸೂಚಿಸುತ್ತದೆ
- ಇದು ಒಳನುಗ್ಗುವವರು, ಉದ್ದೇಶಿತ ದಾಳಿಕೋರರು ಮತ್ತು ಅವಕಾಶವಾದಿ ಮಾಲ್‌ವೇರ್‌ಗಳಿಂದ ಕಂಪ್ಯೂಟರ್ ನೆಟ್‌ವರ್ಕ್‌ಗಳನ್ನು ಸುರಕ್ಷಿತಗೊಳಿಸಲು ಸಂಸ್ಥೆಗಳನ್ನು ಸಕ್ರಿಯಗೊಳಿಸುವ ತಂತ್ರವಾಗಿದೆ.
- ನವೀಕರಿಸಿದ ನೆಟ್‌ವರ್ಕ್ ಸುರಕ್ಷತೆಯ ವಿಧಾನಗಳು:
    1. ಹೆಚ್ಚುವರಿ ಲಾಗಿನ್‌ಗಳು
    2. ಹೊಸ ಪಾಸ್‌ವರ್ಡ್‌ಗಳು
    3. ಆಂಟಿವೈರಸ್ ಕಾರ್ಯಕ್ರಮಗಳು
    4. ಫೈರ್ವಾಲ್ಗಳು

5. ಆಂಟಿಸೈವೇರ್ ಸಾಫ್ಟ್‌ವೇರ್

6. ಇಂಟರ್ನೆಟ್ ಪ್ರವೇಶವನ್ನು ಮೇಲ್ವಿಚಾರಣೆ ಮಾಡಲಾಗಿದೆ

7. ಗೂಢಲಿಪೀಕರಣ

4. ಕ್ಲೌಡ್ ಭದ್ರತೆ

- ಕ್ಲೌಡ್ ಸೆಕ್ಯುರಿಟಿ ಎನ್ನುವುದು ಸಾಫ್ಟ್‌ವೇರ್ ಆಧಾರಿತ ಭದ್ರತಾ ಸಾಧನವಾಗಿದ್ದು, ಅದು ಕ್ಲೌಡ್ ಸಂಪನ್ಮೂಲಗಳಲ್ಲಿನ ಡೇಟಾವನ್ನು ರಕ್ಷಿಸುತ್ತದೆ ಮತ್ತು ಮೇಲ್ವಿಚಾರಣೆ ಮಾಡುತ್ತದೆ
- ಎಂಟರ್‌ಪ್ರೈಸ್ ಬಳಕೆದಾರರಿಗೆ ತಮ್ಮ ಡೇಟಾವನ್ನು ಉತ್ತಮವಾಗಿ ಸುರಕ್ಷಿತಗೊಳಿಸಲು ಸಹಾಯ ಮಾಡಲು ಕ್ಲೌಡ್ ಪೂರೈಕೆದಾರರು ನಿರಂತರವಾಗಿ ಹೊಸ ಭದ್ರತಾ ಪರಿಕರಗಳನ್ನು ರಚಿಸುತ್ತಿದ್ದಾರೆ ಮತ್ತು ಕಾರ್ಯಗತಗೊಳಿಸುತ್ತಿದ್ದಾರೆ
- ಕ್ಲೌಡ್ ಸೆಕ್ಯುರಿಟಿಯು ಡೇಟಾ ಸೆಂಟರ್‌ನಲ್ಲಿ ಸಂಗ್ರಹವಾಗಿರುವ ವ್ಯಾಪಾರ ಸೇವೆಗಳನ್ನು ಸಹ ಒಳಗೊಂಡಿರಬಹುದು

5.ಇಂಟರ್ನೆಟ್ ಆಫ್ ಥಿಂಗ್ಸ್ (IOT) ಭದ್ರತೆ

- IOT ಭದ್ರತೆಯು ಇಂಟರ್ನೆಟ್-ಸಂಪರ್ಕಿತ ಅಥವಾ ನೆಟ್‌ವರ್ಕ್ ಆಧಾರಿತ ಸಾಧನಗಳನ್ನು ಸುರಕ್ಷಿತಗೊಳಿಸಲು ಬಳಸುವ ರಕ್ಷಣೆಯ ವಿಧಾನಗಳನ್ನು ಸೂಚಿಸುತ್ತದೆ
- I OT ಭದ್ರತೆಯು ಇಂಟರ್ನೆಟ್ ಆಫ್ ಥಿಂಗ್ಸ್ (IOT) ನಲ್ಲಿ ಸಂಪರ್ಕಿತ ಸಾಧನಗಳು ಮತ್ತು ನೆಟ್‌ವರ್ಕ್‌ಗಳನ್ನು ರಕ್ಷಿಸುವ ತಂತ್ರಜ್ಞಾನ ವಿಭಾಗವಾಗಿದೆ.

Q5. ಸೈಬರ್ ಭದ್ರತೆಯ ಅಗತ್ಯ ಅಂಶಗಳನ್ನು ವಿವರಿಸಿ

ಸೈಬರ್ ಭದ್ರತೆಯ ಐದು ಅಗತ್ಯ ಅಂಶಗಳು:

1. ಪರಿಣಾಮಕಾರಿ ಚೌಕಟ್ಟು
2. ಎಂಡ್-ಟು-ಎಂಡ್ ಸೊಕ್ಕೇಪ್
3. ಸಂಪೂರ್ಣ ಅಪಾಯದ ಮೌಲ್ಯಮಾಪನ ಮತ್ತು ಬೆದರಿಕೆ ಮಾಡೆಲಿಂಗ್
4. ಪೂರ್ವಭಾವಿ ಘಟನೆಯ ಪ್ರತಿಕ್ರಿಯೆ ಯೋಜನೆ
5. ಮೀಸಲಾದ ಸೈಬರ್ ಸೆಕ್ಯುರಿಟಿ ಸಂಪನ್ಮೂಲಗಳು

1.ಪರಿಣಾಮಕಾರಿ ಚೌಕಟ್ಟು

- ಒಂದು ಚೌಕಟ್ಟನ್ನು ಅಳವಡಿಸಿಕೊಳ್ಳಬೇಕು, ಸರಿಹೊಂದಿಸಬೇಕು ಮತ್ತು ಸಂಸ್ಥೆಯ ನಿರ್ದಿಷ್ಟ ಸಂದರ್ಭಗಳಿಗೆ ಮತ್ತು ದತ್ತಾಂಶದ ಪ್ರಕಾರವನ್ನು ರಕ್ಷಿಸಬೇಕು.
- ಕಾರ್ಯನಿರ್ವಾಹಕರು ಸಂಸ್ಥೆಯ ಎಲ್ಲಾ ಸಂಪನ್ಮೂಲಗಳಿಗೆ ಅನ್ವಯಿಸುವ ಸರಿಯಾದ ಆಡಳಿತವನ್ನು ಸ್ಥಾಪಿಸುವ ಅಗತ್ಯವಿದೆ - ಅದರ ಜನರು, ಪ್ರಕ್ರಿಯೆಗಳು ಮತ್ತು ತಂತ್ರಜ್ಞಾನ

2.ಎಂಡ್-ಟು-ಎಂಡ್ ಸ್ಕೋಪ್

- ಯಶಸ್ವಿಯಾಗಲು ಸೈಬರ್ ಭದ್ರತಾ ಕಾರ್ಯಕ್ರಮವು ಸಮಗ್ರವಾಗಿರಬೇಕು - ಅಂದರೆ, ಸಂರಕ್ಷಿಸಬೇಕಾದ ಸಂಸ್ಥೆಯಲ್ಲಿನ ಎಲ್ಲಾ ಡೇಟಾವನ್ನು ಪರಿಹರಿಸಿ

3. ಸಂಪೂರ್ಣ ಅಪಾಯದ ಮೌಲ್ಯಮಾಪನ ಮತ್ತು ಬೆದರಿಕೆ ಮಾಡೆಲಿಂಗ್

- ಅಪಾಯಗಳನ್ನು ಗುರುತಿಸುವುದು ಮತ್ತು ಬೆದರಿಕೆಗಳ ಒಂದು ಶ್ರೇಣಿಯ ಸಂಭವನೀಯತೆ ಮತ್ತು ಅವರು ಮಾಡಬಹುದಾದ ಹಾನಿ ಸೈಬರ್ ಭದ್ರತಾ ಬೆದರಿಕೆಗಳಿಗೆ ಆದ್ಯತೆ ನೀಡುವ ನಿರ್ಣಾಯಕ ಹಂತವಾಗಿದೆ

4.ಪ್ರೊಆಕ್ಟಿವ್ ಘಟನೆಯ ಪ್ರತಿಕ್ರಿಯೆ ಯೋಜನೆ

- ಯಾವುದೇ ವ್ಯವಸ್ಥೆಯ ಭದ್ರತೆಯನ್ನು ಅಂತಿಮವಾಗಿ ಉಲ್ಲಂಘಿಸಬಹುದು ಎಂದು ಒಪ್ಪಿಕೊಂಡು, ಅನೇಕ ಸಂಸ್ಥೆಗಳು ಘಟನೆ ಪ್ರತಿಕ್ರಿಯೆ ಯೋಜನೆಗಳನ್ನು ಅಳವಡಿಸಿಕೊಂಡಿವೆ

5. ಡೆಡಿಕೇಟೆಡ್ ಸೈಬರ್ ಸೆಕ್ಯುರಿಟಿ ಸಂಪನ್ಮೂಲಗಳು

- ನಿರ್ಣಾಯಕ ಅಂಶವೆಂದರೆ ಸಂಸ್ಥೆಯ ಸೈಬರ್ ಭದ್ರತೆಯನ್ನು ನಿರ್ವಹಿಸಲು ಮೀಸಲಾಗಿರುವ ಸಿಬ್ಬಂದಿ

Q6. ಸೈಬರ್ ಬೆದರಿಕೆ ಎಂದರೇನು?

- ಸೈಬರ್ ಬೆದರಿಕೆ ಅಥವಾ ಸೈಬರ್ ಭದ್ರತಾ ಬೆದರಿಕೆಯು ದುರುದ್ದೇಶಪೂರಿತ ಕ್ರಿಯೆಯಾಗಿದ್ದು ಅದು ಡೇಟಾವನ್ನು ಹಾನಿ ಮಾಡಲು, ಡೇಟಾವನ್ನು ಕದಿಯಲು ಅಥವಾ ಡಿಜಿಟಲ್ ಜೀವನವನ್ನು ಅಡ್ಡಿಪಡಿಸಲು ಪ್ರಯತ್ನಿಸುತ್ತದೆ.
- ಸೈಬರ್ ಬೆದರಿಕೆಗಳಲ್ಲಿ ಕಂಪ್ಯೂಟರ್ ವೈರಸ್‌ಗಳು, ಡೇಟಾ ಉಲ್ಲಂಘನೆಗಳು , ಸೇವೆಯ ನಿರಾಕರಣೆ (D O S) ದಾಳಿಗಳು ಮತ್ತು ಇತರ ದಾಳಿ ವೆಕ್ಟರ್ ಸೇರಿವೆ
- ಸೈಬರ್ ಬೆದರಿಕೆಯು ಮಾಹಿತಿ ತಂತ್ರಜ್ಞಾನ ಸ್ವತ್ತು, ಕಂಪ್ಯೂಟರ್ ನೆಟ್‌ವರ್ಕ್, ಬೌದ್ಧಿಕ ಆಸ್ತಿ ಅಥವಾ ಸೂಕ್ಷ್ಮ ಡೇಟಾವನ್ನು ಅನಧಿಕೃತ ಪ್ರವೇಶ, ಹಾನಿ, ಅಡ್ಡಿ ಅಥವಾ ಕದಿಯುವ ಗುರಿಯನ್ನು ಹೊಂದಿರುವ ಸೈಬರ್ ದಾಳಿಯನ್ನು ಉಲ್ಲೇಖಿಸುತ್ತದೆ.

Q7. ಸೈಬರ್ ಭದ್ರತಾ ಬೆದರಿಕೆಗಳ ಪ್ರಕಾರಗಳು ಯಾವುವು?

1. ಮಾಲ್ವೇರ್. ಮಾಲ್‌ವೇರ್ ಎಂಬುದು ಸ್ಪೈವೇರ್, ರಾನ್ಸಮ್‌ವೇರ್, ವೈರಸ್‌ಗಳು ಮತ್ತು ವರ್ಮ್‌ಗಳಂತಹ ದುರುದ್ದೇಶಪೂರಿತ ಸಾಫ್ಟ್‌ವೇರ್ ಆಗಿದೆ
2. ಎಮೋಟೆಟ್
3. ಸೇವೆಯ ನಿರಾಕರಣೆ
4. ಮಧ್ಯದಲ್ಲಿ ಮನುಷ್ಯ
5. ಫಿಶಿಂಗ್
6. SQL ಇಂಜೆಕ್ಷನ್
7. ಪಾಸ್ವರ್ಡ್ ದಾಳಿಗಳು

Q8. ಸೈಬರ್ ಭದ್ರತೆಗಾಗಿ ಪರಿಕರಗಳನ್ನು ವಿವರಿಸಿ

ಸೈಬರ್ ಭದ್ರತೆಗಾಗಿ ಪರಿಕರಗಳು:

1.ಪಾಸ್‌ವರ್ಡ್ ನಿರ್ವಾಹಕರು

2. ವರ್ಚುವಲ್ ಪ್ರೈವೇಟ್ ನೆಟ್‌ವರ್ಕ್ (VPN)

3. ಬ್ಲಾಕ್‌ಚೈನ್ ತಂತ್ರಜ್ಞಾನ

1.ಪಾಸ್‌ವರ್ಡ್ ನಿರ್ವಾಹಕರು

- ಪಾಸ್‌ವರ್ಡ್ ನಿರ್ವಾಹಕವು ಆನ್‌ಲೈನ್ ರುಜುವಾತುಗಳನ್ನು ಸಂಗ್ರಹಿಸಲು ಮತ್ತು ನಿರ್ವಹಿಸಲು ವಿನ್ಯಾಸಗೊಳಿಸಲಾದ ಸಾಫ್ಟ್‌ವೇರ್ ಅಪ್ಲಿಕೇಶನ್ ಆಗಿದೆ. ಸಾಮಾನ್ಯವಾಗಿ, ಈ ಪಾಸ್‌ವರ್ಡ್‌ಗಳನ್ನು ಎನ್‌ಕ್ರಿಪ್ಟ್ ಮಾಡಿದ ಡೇಟಾಬೇಸ್‌ನಲ್ಲಿ ಸಂಗ್ರಹಿಸಲಾಗುತ್ತದೆ ಮತ್ತು ಮಾಸ್ಟರ್ ಪಾಸ್‌ವರ್ಡ್‌ನ ಹಿಂದೆ ಲಾಕ್ ಮಾಡಲಾಗುತ್ತದೆ
- ಪಾಸ್‌ವರ್ಡ್ ನಿರ್ವಾಹಕವು ಮೂರನೇ ವ್ಯಕ್ತಿಯಾಗಿದ್ದು ಅದು ನಿಮ್ಮ ನೆಟ್‌ವರ್ಕ್‌ನಾದ್ಯಂತ ಬಳಕೆದಾರರಿಗೆ ಮಾಸ್ಟರ್ ಪಾಸ್‌ವರ್ಡ್ ಅನ್ನು ರಚಿಸುತ್ತದೆ
- ಪಾಸ್‌ವರ್ಡ್ ನಿರ್ವಾಹಕರು ನಿಮಗೆ ಅನನ್ಯ ಮತ್ತು ಬಲವಾದ ಪಾಸ್‌ವರ್ಡ್‌ಗಳನ್ನು ರಚಿಸಲು ಸಹಾಯ ಮಾಡುತ್ತಾರೆ, ಅವುಗಳನ್ನು ಒಂದು ಸುರಕ್ಷಿತ (ಎನ್‌ಕ್ರಿಪ್ಟ್ ಮಾಡಿದ) ಸ್ಥಳದಲ್ಲಿ ಸಂಗ್ರಹಿಸಿ ಮತ್ತು ಕೇವಲ ಒಂದು ಮಾಸ್ಟರ್ ಪಾಸ್‌ವರ್ಡ್ ಅನ್ನು ನೆನಪಿಟ್ಟುಕೊಳ್ಳುವ ಅಗತ್ಯವಿರುವಾಗ ಅವುಗಳನ್ನು ಬಳಸಿ
- ಮಾಸ್ಟರ್ ಪಾಸ್‌ವರ್ಡ್ ನಿಮ್ಮ ಎನ್‌ಕ್ರಿಪ್ಟ್ ಮಾಡಿದ ವಾಲ್ಟ್ ಅನ್ನು ಅನ್‌ಲಾಕ್ ಮಾಡುತ್ತದೆ ಅದು ನಿಮ್ಮ ಪ್ರತಿಯೊಂದು ಪಾಸ್‌ವರ್ಡ್‌ಗಳಿಗೆ ಪ್ರವೇಶವನ್ನು ನೀಡುತ್ತದೆ
- ಪಾಸ್‌ವರ್ಡ್ ನಿರ್ವಾಹಕರನ್ನು ಟ್ರ್ಯಾಕ್ ಮಾಡಲು ಮತ್ತು ಸುರಕ್ಷಿತ ಪಾಸ್‌ವರ್ಡ್‌ಗಳನ್ನು ರಚಿಸಲು ಬಳಸಲಾಗುತ್ತಿದೆ. ಬಳಕೆದಾರರು ಪಾಸ್‌ವರ್ಡ್ ನಿರ್ವಾಹಕರ ಒಂದು ಪಾಸ್‌ವರ್ಡ್ ಅನ್ನು ಮಾತ್ರ ನೆನಪಿಟ್ಟುಕೊಳ್ಳಬೇಕು

- Lastpass, Dashlane, Sticky Password ಮತ್ತು KeepassX ನಂತಹ ಪಾಸ್‌ವರ್ಡ್ ನಿರ್ವಾಹಕರನ್ನು ಬಳಸಬಹುದು

2. ವರ್ಚುವಲ್ ಪ್ರೈವೇಟ್ ನೆಟ್‌ವರ್ಕ್ (VPN)

- VPN ಎಂದರೆ **"ವರ್ಚುವಲ್ ಪ್ರೈವೇಟ್ ನೆಟ್‌ವರ್ಕ್"** ಮತ್ತು ಸಾರ್ವಜನಿಕ ನೆಟ್‌ವರ್ಕ್‌ಗಳನ್ನು ಬಳಸುವಾಗ ಸಂರಕ್ಷಿತ ನೆಟ್‌ವರ್ಕ್ ಸಂಪರ್ಕವನ್ನು ಸ್ಥಾಪಿಸುವ ಅವಕಾಶವನ್ನು ವಿವರಿಸುತ್ತದೆ. VPN ಗಳು ನಿಮ್ಮ ಇಂಟರ್ನೆಟ್ ಟ್ರಾಫಿಕ್ ಅನ್ನು ಎನ್‌ಕ್ರಿಪ್ಟ್ ಮಾಡುತ್ತದೆ ಮತ್ತು ನಿಮ್ಮ ಆನ್‌ಲೈನ್ ಗುರುತನ್ನು ಮರೆಮಾಚುತ್ತದೆ
- ಇಂಟರ್ನೆಟ್ ನಡುವೆ ಸುರಕ್ಷಿತ ಸಂಪರ್ಕವನ್ನು ಸ್ಥಾಪಿಸುತ್ತದೆ . VPN ಮೂಲಕ, ನಿಮ್ಮ ಎಲ್ಲಾ ಡೇಟಾ ಟ್ರಾಫಿಕ್ ಅನ್ನು ಎನ್‌ಕ್ರಿಪ್ಟ್ ಮಾಡಿದ ವರ್ಚುವಲ್ ಟನಲ್ ಮೂಲಕ ರವಾನಿಸಲಾಗುತ್ತದೆ
- ನೀವು ಇಂಟರ್ನೆಟ್ ಅನ್ನು ಬಳಸುವಾಗ ಇದು ನಿಮ್ಮ IP ವಿಳಾಸವನ್ನು ಮರೆಮಾಚುತ್ತದೆ , ಅದರ ಸ್ಥಳವು ಎಲ್ಲರಿಗೂ ಗೋಚರಿಸುವುದಿಲ್ಲ. ನೀವು ಇನ್ನೂ VPN ಬಳಸಿಕೊಂಡು ಎಲ್ಲಾ ಆನ್‌ಲೈನ್ ಸೇವೆಗಳನ್ನು ಪ್ರವೇಶಿಸಬಹುದು
- *VPN* ಹೋಸ್ಟ್‌ನಿಂದ ವಿಶೇಷವಾಗಿ ಕಾನ್ಫಿಗರ್ ಮಾಡಲಾದ ರಿಮೋಟ್ ಸರ್ವರ್ ಮೂಲಕ ನೆಟ್‌ವರ್ಕ್ ಮರುನಿರ್ದೇಶಿಸಲು ಅನುಮತಿಸುವ ಮೂಲಕ VPN ನಿಮ್ಮ IP ವಿಳಾಸವನ್ನು ಮರೆಮಾಡುತ್ತದೆ.
- ಇದರರ್ಥ ನೀವು VPN ನೊಂದಿಗೆ ಆನ್‌ಲೈನ್‌ನಲ್ಲಿ ಸರ್ಫ್ ಮಾಡಿದರೆ, *VPN* ಸರ್ವರ್ ನಿಮ್ಮ ಡೇಟಾದ ಮೂಲವಾಗುತ್ತದೆ
- VPN ಸಂಪರ್ಕವು ನಿಮ್ಮ ಡೇಟಾ ದಟ್ಟಣೆಯನ್ನು ಆನ್‌ಲೈನ್‌ನಲ್ಲಿ ಮರೆಮಾಚುತ್ತದೆ ಮತ್ತು ಬಾಹ್ಯ ಪ್ರವೇಶದಿಂದ ಅದನ್ನು ರಕ್ಷಿಸುತ್ತದೆ
- ಡೇಟಾ ಸೋರಿಕೆಗಳು ಮತ್ತು ಸೈಬರ್‌ಅಟ್ಯಾಕ್‌ಗಳಿಂದ ರಕ್ಷಿಸಲು ನೀವು ಯಾವಾಗಲೂ VPN ಅನ್ನು ಆನ್ ಮಾಡಬೇಕು

3. ಬ್ಲಾಕ್‌ಚೈನ್ ತಂತ್ರಜ್ಞಾನ

- ಬ್ಲಾಕ್‌ಚೈನ್ ತಂತ್ರಜ್ಞಾನವು ವಿಕೇಂದ್ರೀಕೃತ ಮತ್ತು ವಿತರಿಸಿದ ಲೆಡ್ಜರ್ ವ್ಯವಸ್ಥೆಯಾಗಿದ್ದು ಅದು ಬಹು ಕಂಪ್ಯೂಟರ್‌ಗಳ ನಡುವೆ ವಹಿವಾಟುಗಳನ್ನು ದಾಖಲಿಸಬಹುದು
- Blockchain ಬಿಟ್‌ಕಾಯಿನ್‌ನ ಹಿಂದಿನ ತಂತ್ರಜ್ಞಾನವಾಗಿ ಪ್ರಾರಂಭವಾಯಿತು ಆದರೆ ಸೈಬರ್ ಸೆಕ್ಯುರಿಟಿಗಾಗಿ ಭರವಸೆಯ ತಗ್ಗಿಸುವ ತಂತ್ರಜ್ಞಾನವಾಗಿ ಜನಪ್ರಿಯವಾಗಿ ಬೆಳೆದಿದೆ
- ಮೊದಲ ಕ್ರಿಪ್ಟೋಕರೆನ್ಸಿಯಾಗಿದೆ
- ಬ್ಲಾಕ್‌ಚೈನ್ ತಂತ್ರಜ್ಞಾನವು ವಿತರಿಸಿದ ನೆಟ್‌ವರ್ಕ್‌ನಾದ್ಯಂತ ಸದಸ್ಯರ ಭಾಗವಹಿಸುವಿಕೆಯ ಮೂಲಕ ವಿಕೇಂದ್ರೀಕರಣವನ್ನು ಸಕ್ರಿಯಗೊಳಿಸುತ್ತದೆ

- ಬ್ಲಾಕ್‌ಚೈನ್ ಡೇಟಾ ಸಂಗ್ರಹಣೆಯನ್ನು ಸಂಪೂರ್ಣವಾಗಿ ಸ್ವಯಂಚಾಲಿತಗೊಳಿಸುತ್ತದೆ ಆದ್ದರಿಂದ ಈ ಡೇಟಾ ಸಂಗ್ರಹಣಾ ವ್ಯವಸ್ಥೆಗಳಲ್ಲಿ ಮಾನವ ಅಂಶವನ್ನು ಕಡಿಮೆ ಮಾಡುತ್ತದೆ

Q9. ಸೈಬರ್ ದಾಳಿ ಎಂದರೇನು?

- ಅನಧಿಕೃತ ಪ್ರವೇಶ, ಅನುಮೋದಿಸದ ಬದಲಾವಣೆಗಳು ಮತ್ತು ದುರುದ್ದೇಶಪೂರಿತ ವಿನಾಶ ಸೇರಿದಂತೆ ನೆಟ್‌ವರ್ಕ್ ಮಾಡಲಾದ ಕಂಪ್ಯೂಟರ್‌ಗಳು ಮತ್ತು ಅವುಗಳ ಸಂಬಂಧಿತ ಸಂಪನ್ಮೂಲಗಳ ಕಾರ್ಯಗಳನ್ನು ದುರ್ಬಲಗೊಳಿಸುವ ಉದ್ದೇಶವನ್ನು ಹೊಂದಿರುವ ದುರುದ್ದೇಶಪೂರಿತ ನಟನ ಆಕ್ರಮಣಕಾರಿ ಕ್ರಿಯೆ
- ಸೈಬರ್ ದಾಳಿಯು ಬೆದರಿಕೆ ನಟರು ನಡೆಸುವ ಕ್ರಿಯೆಗಳ ಒಂದು ಗುಂಪಾಗಿದೆ, ಅವರು ಅನಧಿಕೃತ ಪ್ರವೇಶವನ್ನು ಪಡೆಯಲು ಪ್ರಯತ್ನಿಸುತ್ತಾರೆ, ಡೇಟಾವನ್ನು ಕದಿಯುತ್ತಾರೆ ಅಥವಾ ಕಂಪ್ಯೂಟರ್‌ಗಳು, ಕಂಪ್ಯೂಟರ್ ನೆಟ್‌ವರ್ಕ್‌ಗಳು ಅಥವಾ ಇತರ ಕಂಪ್ಯೂಟಿಂಗ್ ವ್ಯವಸ್ಥೆಗಳಿಗೆ ಹಾನಿಯನ್ನುಂಟುಮಾಡುತ್ತಾರೆ.
- ಕಂಪ್ಯೂಟರ್ ಮಾಹಿತಿ ವ್ಯವಸ್ಥೆಗಳು , ಕಂಪ್ಯೂಟರ್ ಜಾಲಗಳು , ಮೂಲಸೌಕರ್ಯಗಳು ಅಥವಾ ವೈಯಕ್ತಿಕ ಕಂಪ್ಯೂಟರ್ ಸಾಧನಗಳನ್ನು ಗುರಿಯಾಗಿಸುವ ಯಾವುದೇ ಆಕ್ರಮಣಕಾರಿ ತಂತ್ರವಾಗಿದೆ
- ಸೈಬರ್-ದಾಳಿಗಳ ಉದಾಹರಣೆಗಳಲ್ಲಿ ಡಿಸ್ಟ್ರಿಬ್ಯೂಟೆಡ್ ಡಿನೈಯಲ್ ಆಫ್ ಸರ್ವಿಸ್ (DDOS) ಮತ್ತು ಮ್ಯಾನ್-ಇನ್-ದಿ-ಮಿಡಲ್ (MITM) ದಾಳಿಗಳು ಸೇರಿವೆ.

Q10. ಸೈಬರ್ ದಾಳಿ, ಸೈಬರ್ ಬೆದರಿಕೆ ಮತ್ತು ಸೈಬರ್ ಅಪಾಯದ ಪದಗಳ ನಡುವಿನ ವ್ಯತ್ಯಾಸವೇನು?

- ಸೈಬರ್ ದಾಳಿ, ಸೈಬರ್ ಬೆದರಿಕೆ ಮತ್ತು ಸೈಬರ್ ಅಪಾಯದ ಪದಗಳು ಈ ಕೆಳಗಿನಂತೆ ಪರಸ್ಪರ ಸಂಬಂಧ ಹೊಂದಿವೆ. ಸೈಬರ್-ದಾಳಿಯು ಆಕ್ರಮಣಕಾರಿ ಕ್ರಿಯೆಯಾಗಿದೆ, ಆದರೆ ಸೈಬರ್-ಬೆದರಿಕೆಯು ನಿರ್ದಿಷ್ಟ ದಾಳಿಯು ಸಂಭವಿಸುವ ಸಾಧ್ಯತೆಯಾಗಿದೆ, ಮತ್ತು ವಿಷಯದ ಬೆದರಿಕೆಗೆ ಸಂಬಂಧಿಸಿದ ಸೈಬರ್ ಅಪಾಯವು ಸಂಭವನೀಯ ನಷ್ಟಗಳ ಸಂಭವನೀಯತೆಯನ್ನು ಅಂದಾಜು ಮಾಡುತ್ತದೆ
- ಉದಾಹರಣೆಗೆ, ಬೋಟ್‌ನೆಟ್‌ನಿಂದ ಡಿಸ್ಟ್ರಿಬ್ಯೂಟೆಡ್ ಡಿನೈಯಲ್ ಆಫ್ ಸರ್ವಿಸ್ (DDOS) ಸೈಬರ್-ದಾಳಿಯು ಉದ್ಯಮಗಳಿಗೆ ಸೈಬರ್-ಬೆದರಿಕೆಯಾಗಿದೆ, ಸೈಬರ್ ಅಪಾಯವು ವೆಬ್‌ಸೈಟ್ ಡೌನ್‌ಟೈಮ್ ಮತ್ತು DDOS ಸೈಬರ್-ದಾಳಿ ಸಂಭವಿಸುವ ಸಂಭವನೀಯತೆಯಿಂದಾಗಿ ಕಳೆದುಹೋದ ಆದಾಯದ ಕಾರ್ಯವಾಗಿದೆ.

Q11. ಮಾಲ್ವೇರ್ ಎಂದರೇನು?

ಮಾಲ್‌ವೇರ್ ಒಳನುಗ್ಗುವ ಸಾಫ್ಟ್‌ವೇರ್ ಆಗಿದ್ದು ಅದು ಕಂಪ್ಯೂಟರ್‌ಗಳು ಮತ್ತು ನೆಟ್‌ವರ್ಕ್‌ಗಳನ್ನು ಹಾನಿಗೊಳಿಸಲು ಮತ್ತು ನಾಶಮಾಡಲು ವಿನ್ಯಾಸಗೊಳಿಸಲಾಗಿದೆ

Q12. ಸೈಬರ್ ದಾಳಿಯ ವಿಧಗಳನ್ನು ವಿವರಿಸಿ

ಸೈಬರ್ ದಾಳಿಯ ವಿಧಗಳು

1. ಮಾಲ್ವೇರ್ ದಾಳಿ
2. ಸೇವೆಯ ನಿರಾಕರಣೆ ದಾಳಿ
3. ಮಧ್ಯಮ ದಾಳಿಯಲ್ಲಿ ಮನುಷ್ಯ
4. ಫಿಶಿಂಗ್ ದಾಳಿ
5. SQL ಇಂಜೆಕ್ಷನ್ ದಾಳಿ
6. ಪಾಸ್ವರ್ಡ್ ದಾಳಿ
7. IOT ದಾಳಿ

1. ಮಾಲ್ವೇರ್ ದಾಳಿ

- ಇದು ಸೈಬರ್‌ದಾಕ್‌ಗಳ ಸಾಮಾನ್ಯ ವಿಧಗಳಲ್ಲಿ ಒಂದಾಗಿದೆ. "ಮಾಲ್ವೇರ್" ವರ್ಮ್‌ಗಳು, ವೈರಸ್, ransomware, ಆಡ್‌ವೇರ್ ಮತ್ತು ಟ್ರೋಜನ್‌ಗಳು ಸೇರಿದಂತೆ ದುರುದ್ದೇಶಪೂರಿತ ಸಾಫ್ಟ್‌ವೇರ್ ವೈರಸ್‌ಗಳನ್ನು ಸೂಚಿಸುತ್ತದೆ

2. ಫಿಶಿಂಗ್ ಅಟ್ಯಾಕ್

- ಇದು ಒಂದು ರೀತಿಯ ಸಾಮಾಜಿಕ ಇಂಜಿನಿಯರಿಂಗ್ ದಾಳಿಯಾಗಿದ್ದು, ಇದರಲ್ಲಿ ಆಕ್ರಮಣಕಾರನು ವಿಶ್ವಾಸಾರ್ಹ ಸಂಪರ್ಕಕ್ಕೆ ಸೋಗು ಹಾಕುತ್ತಾನೆ ಮತ್ತು ಬಲಿಪಶುವಿಗೆ ನಕಲಿ ಮೇಲ್‌ಗಳನ್ನು ಕಳುಹಿಸುತ್ತಾನೆ
- ಫಿಶಿಂಗ್ ದಾಳಿಗಳು ಸಾಮಾಜಿಕ ನೆಟ್‌ವರ್ಕ್‌ಗಳು ಮತ್ತು ಇತರ ಆನ್‌ಲೈನ್ ಸಮುದಾಯಗಳ ಮೂಲಕವೂ ನಡೆಯಬಹುದು

3. ಮ್ಯಾನ್-ಇನ್-ದಿ-ಮಿಡಲ್ ಅಟ್ಯಾಕ್

- ಈ ದಾಳಿಯಲ್ಲಿ, ಆಕ್ರಮಣಕಾರನು ಎರಡು-ಪಕ್ಷದ ಸಂವಹನದ ನಡುವೆ ಬರುತ್ತಾನೆ, ಅಂದರೆ, ಆಕ್ರಮಣಕಾರನು ಕ್ಲೈಂಟ್ ಮತ್ತು ಹೋಸ್ಟ್ ನಡುವಿನ ಸೆಶನ್ ಅನ್ನು ಹೈಜಾಕ್ ಮಾಡುತ್ತಾನೆ. ಹಾಗೆ ಮಾಡುವುದರಿಂದ, ಹ್ಯಾಕರ್‌ಗಳು ಡೇಟಾವನ್ನು ಕದಿಯುತ್ತಾರೆ ಮತ್ತು ಕುಶಲತೆಯಿಂದ ನಿರ್ವಹಿಸುತ್ತಾರೆ

4. ಸೇವೆಯ ನಿರಾಕರಣೆ (DOS) ದಾಳಿ

- ಸಂಪನ್ಮೂಲಗಳು ಮತ್ತು ಬ್ಯಾಂಡ್‌ವಿಡ್ತ್ ಅನ್ನು ಓವರ್‌ಲೋಡ್ ಮಾಡಲು ಟ್ರಾಫಿಕ್ ನೊಂದಿಗೆ ಸಿಸ್ಟಂಗಳು, ಸರ್ವರ್‌ಗಳು ಮತ್ತು/ಅಥವಾ ನೆಟ್‌ವರ್ಕ್‌ಗಳನ್ನು ಪ್ರವಾಹ ಮಾಡುವ ಮೂಲಕ DOS ದಾಳಿಗಳು ಕಾರ್ಯನಿರ್ವಹಿಸುತ್ತವೆ.
- ಈ ಫಲಿತಾಂಶವು ಸಿಸ್ಟಂ ಅನ್ನು ಪ್ರಕ್ರಿಯೆಗೊಳಿಸಲು ಮತ್ತು ಕಾನೂನುಬದ್ಧ ವಿನಂತಿಗಳನ್ನು ಪೂರೈಸಲು ಸಾಧ್ಯವಾಗುತ್ತಿಲ್ಲ

Q13. ಸೈಬರ್ ದಾಳಿಗಳನ್ನು ತಪ್ಪಿಸಲು ಸಲಹೆಗಳು ಯಾವುವು?

ಸೈಬರ್ ದಾಳಿಯನ್ನು ತಪ್ಪಿಸಲು ಸಲಹೆಗಳು

1 .ಸೈಬರ್ ಭದ್ರತಾ ತತ್ವಗಳಲ್ಲಿ ಉದ್ಯೋಗಿಗಳಿಗೆ ತರಬೇತಿ ನೀಡಿ

2. ಪ್ರತಿ ಕಂಪ್ಯೂಟರ್‌ನಲ್ಲಿ ಆಂಟಿವೈರಸ್ ಮತ್ತು ಆಂಟಿ-ಸ್ಪೈವೇರ್ ಸಾಫ್ಟ್‌ವೇರ್ ಅನ್ನು ಸ್ಥಾಪಿಸಿ, ಬಳಸಿ ಮತ್ತು ನಿಯಮಿತವಾಗಿ ನವೀಕರಿಸಿ

3. ಇಂಟರ್ನೆಟ್ ಸಂಪರ್ಕಕ್ಕಾಗಿ ಫೈರ್‌ವಾಲ್ ಬಳಸಿ

4. ಆಪರೇಟಿಂಗ್ ಸಿಸ್ಟಮ್‌ಗಳು ಮತ್ತು ಅಪ್ಲಿಕೇಶನ್‌ಗಳು ಲಭ್ಯವಾದಂತೆ ಸಾಫ್ಟ್‌ವೇರ್ ಅನ್ನು ಡೌನ್ ಲೋಡ್ ಮಾಡಿ ಮತ್ತು ಸ್ಥಾಪಿಸಿ

5. ಪ್ರಮುಖ ವ್ಯಾಪಾರದ ಡೇಟಾ ಮತ್ತು ಮಾಹಿತಿಯ ಬ್ಯಾಕಪ್ ಪ್ರತಿಗಳನ್ನು ಮಾಡಿ ಸಾಫ್ಟ್‌ವೇರ್ ಅನ್ನು ಸ್ಥಾಪಿಸಲು

6. ಪಾಸ್‌ವರ್ಡ್‌ಗಳನ್ನು ನಿಯಮಿತವಾಗಿ ಬದಲಾಯಿಸಿ

Q14. ಯಾವ ವಿಧಾನಗಳನ್ನು ಬಳಸಲಾಗುತ್ತದೆ ಸೈಬರ್ ದಾಳಿಯನ್ನು ತಡೆಗಟ್ಟುವುದು a ಕಂಪನಿ?

1. ಬೆದರಿಕೆಗಳನ್ನು ಗುರುತಿಸಿ
2. ಸೈಬರ್ ಅಪರಾಧಗಳ ಬಗ್ಗೆ ಎಚ್ಚರದಿಂದಿರಿ
3. ಉದ್ಯೋಗಿಗಳ ಮೇಲೆ ಕಣ್ಣಿಡಿ
4. ಎರಡು ಅಂಶಗಳ ದೃಢೀಕರಣವನ್ನು ಬಳಸಿ
5. ನಿಯಮಿತ ಆಧಾರದ ಮೇಲೆ ಲೆಕ್ಕಪರಿಶೋಧನೆಗಳನ್ನು ನಡೆಸುವುದು
6. ಬಲವಾದ ಸೈನ್-ಆಫ್ ನೀತಿಯನ್ನು ಖಚಿತಪಡಿಸಿಕೊಳ್ಳಿ
7. ಪ್ರಮುಖ ಡೇಟಾವನ್ನು ರಕ್ಷಿಸಿ
8. ಅಪಾಯದ ಮೌಲ್ಯಮಾಪನಗಳನ್ನು ಕೈಗೊಳ್ಳಿ
9. ಸೈಬರ್ ಅಪರಾಧದ ವಿರುದ್ಧ ನಿಮ್ಮ ಕಂಪನಿಯನ್ನು ವಿಮೆ ಮಾಡಿ
10. ಅಪಾಯದ ಅಂಶಗಳ ಬಗ್ಗೆ ಆಳವಾದ ಜ್ಞಾನವನ್ನು ಹೊಂದಿರಿ

5. SQL ಇಂಜೆಕ್ಷನ್ ಅಟ್ಯಾಕ್

- ಒಂದು ಸ್ಟ್ರಕ್ಚರ್ಡ್ ಕ್ವೆರಿ ಲ್ಯಾಂಗ್ವೇಜ್ (SQL) ಇಂಜೆಕ್ಷನ್ ದಾಳಿಯು ಡೇಟಾಬೇಸ್-ಚಾಲಿತ ವೆಬ್‌ಸೈಟ್‌ನಲ್ಲಿ ಹ್ಯಾಕರ್ ಪ್ರಮಾಣಿತ SQL ಪ್ರಶ್ನೆಯನ್ನು ಕುಶಲತೆಯಿಂದ ನಿರ್ವಹಿಸಿದಾಗ ಸಂಭವಿಸುತ್ತದೆ.
- ಆಕ್ರಮಣಕಾರರು ಸರ್ವರ್ ಪ್ರಶ್ನೆ ಭಾಷೆ (SQL) ಅನ್ನು ಬಳಸಿಕೊಂಡು ಸರ್ವರ್‌ಗೆ ದುರುದ್ದೇಶಪೂರಿತ ಕೋಡ್ ಅನ್ನು ಸೇರಿಸಿದಾಗ ಇದು ಸಂರಕ್ಷಿತ ಮಾಹಿತಿಯನ್ನು ತಲುಪಿಸಲು ಸರ್ವರ್ ಅನ್ನು ಒತ್ತಾಯಿಸಿದಾಗ ಸಂಭವಿಸುತ್ತದೆ.

6. ಪಾಸ್ವರ್ಡ್ ದಾಳಿ

- ಇದು ದಾಳಿಯ ಒಂದು ರೂಪವಾಗಿದ್ದು ಇದರಲ್ಲಿ ಹ್ಯಾಕರ್ ನಿಮ್ಮ ಪಾಸ್‌ವರ್ಡ್ ಅನ್ನು ವಿವಿಧ ಪ್ರೋಗ್ರಾಂಗಳು ಮತ್ತು ಬ್ರೂಟ್‌ಫೋರ್ಸ್ , ಕೇನ್, ಅಬೆಲ್, ಜಾನ್ ದಿ ರಿಪ್ಪರ್, ಹ್ಯಾಶ್‌ಕ್ಯಾಟ್ ಮುಂತಾದ ಪಾಸ್‌ವರ್ಡ್ ಕ್ರ್ಯಾಕಿಂಗ್ ಸಾಧನಗಳೊಂದಿಗೆ ಭೇದಿಸುತ್ತಾನೆ.

7. ಇಂಟರ್ನೆಟ್ ಆಫ್ ಥಿಂಗ್ಸ್ (IOT) ದಾಳಿಗಳು

- ಈ ದಾಳಿಯಲ್ಲಿ, ದಾಳಿಕೋರರು ಉದ್ದೇಶಿತ ನೆಟ್‌ವರ್ಕ್‌ಗಳನ್ನು ಮೇಲ್ವಿಚಾರಣೆ ಮಾಡಬಹುದು ಮತ್ತು ಭದ್ರತಾ ಲೋಪದೋಷಗಳು ಮತ್ತು IOT ಸಾಧನಗಳು ಮತ್ತು ಸರ್ವರ್ ನಡುವಿನ ದುರ್ಬಲ ಸಂಪರ್ಕಗಳನ್ನು ಬಳಸಿಕೊಳ್ಳುವ ಮೂಲಕ ವೈಯಕ್ತಿಕ ಡೇಟಾವನ್ನು ಕದಿಯಬಹುದು.

1. ಬೆದರಿಕೆಗಳನ್ನು ಗುರುತಿಸಿ

- ನಿಮ್ಮ ವ್ಯಾಪಾರಕ್ಕೆ ಸಂಭವನೀಯ ಬೆದರಿಕೆಗಳನ್ನು ಮೊದಲು ಗುರುತಿಸಿ ಮತ್ತು ವ್ಯವಹರಿಸಿ ಹಾನಿ ಉಂಟುಮಾಡುತ್ತವೆ

2. ಸೈಬರ್ ಅಪರಾಧಗಳ ಬಗ್ಗೆ ಎಚ್ಚರದಿಂದಿರಿ

- ಅದರ ದಾಖಲೆಗಳನ್ನು ಯಾವಾಗಲೂ ಇಟ್ಟುಕೊಳ್ಳಿ ಮಾಹಿತಿಯು ಅಪರಾಧಿಗಳಿಗೆ ಆಕರ್ಷಕವಾಗಿದೆ ಮತ್ತು ಅದು ಅಲ್ಲ

3.ಉದ್ಯೋಗಿಗಳ ಮೇಲೆ ಕಣ್ಣಿಡಿ

- ಉದ್ಯೋಗಿಗಳನ್ನು ಪ್ರೇರೇಪಿಸುವಂತೆ ಇರಿಸಿಕೊಳ್ಳಿ ಮತ್ತು ನಿರ್ಣಾಯಕವಾಗಿ ಸೋರಿಕೆಯಾಗದಂತೆ ಅವರನ್ನು ನಿರುತ್ಸಾಹಗೊಳಿಸಿ ಮಾಹಿತಿ, ಅವರನ್ನು ಕಂಪನಿಗೆ ಹೆಚ್ಚು ನಿಷ್ಠರನ್ನಾಗಿಸಲು ಪ್ರಯತ್ನಿಸಿ

4.ಎರಡು ಅಂಶಗಳ ದೃಢೀಕರಣವನ್ನು ಬಳಸಿ

- ಎರಡು ಅಂಶದ ದೃಢೀಕರಣವನ್ನು ಬಳಸಲು ಎಲ್ಲಾ ಉದ್ಯೋಗಿಗಳನ್ನು ಪ್ರೋತ್ಸಾಹಿಸಿ ಏಕೆಂದರೆ ಇದು ಸೇರಿಸುವ ಮೂಲಕ ಭದ್ರತೆಯನ್ನು ಹೆಚ್ಚಿಸುತ್ತದೆ ಖಾತೆಗಳನ್ನು ಪ್ರವೇಶಿಸಲು ಹೆಚ್ಚುವರಿ ಹಂತ

5. ನಿಯಮಿತ ಆಧಾರದ ಮೇಲೆ ಆಡಿಟ್‌ಗಳನ್ನು ನಡೆಸುವುದು

- ಒಂದು ಮಾಡಬಹುದು ನಿಮ್ಮ ಡೇಟಾವನ್ನು ರಕ್ಷಿಸುವಲ್ಲಿ ಪರಿಣಿತರಾಗಿರುವ ಸೈಬರ್ ಭದ್ರತಾ ಸಲಹೆಗಾರರು ನಡೆಸಿದ ಆಡಿಟ್ ಅನ್ನು ಹೊಂದಿರಿ

Q15.ಫೈರ್‌ವಾಲ್ ಎಂದರೇನು?

- ಫೈರ್‌ವಾಲ್ ಎನ್ನುವುದು ನೆಟ್‌ವರ್ಕ್ ಭದ್ರತಾ ವ್ಯವಸ್ಥೆಯಾಗಿದ್ದು ಅದು ಒಳಬರುವ ಮತ್ತು ಹೊರಹೋಗುವ ನೆಟ್‌ವರ್ಕ್ ಸಂದೇಶ ದಟ್ಟಣೆಯನ್ನು ಮೇಲ್ವಿಚಾರಣೆ ಮಾಡುತ್ತದೆ ಮತ್ತು ನವೀಕರಿಸಬಹುದಾದ ನಿಯಮಗಳ ಆಧಾರದ ಮೇಲೆ ದುರುದ್ದೇಶಪೂರಿತ ಸಂದೇಶಗಳ ಪ್ರಸರಣವನ್ನು ತಡೆಯುತ್ತದೆ

Q16.ಫೈರ್‌ವಾಲ್ ಹೇಗೆ ಕೆಲಸ ಮಾಡುತ್ತದೆ?

- ಫೈರ್‌ವಾಲ್‌ಗಳು ವಿಶ್ವಾಸಾರ್ಹ, ಸುರಕ್ಷಿತ ಆಂತರಿಕ ನೆಟ್‌ವರ್ಕ್ ಮತ್ತು ಬಾಹ್ಯ ನೆಟ್‌ವರ್ಕ್‌ಗಳ ನಡುವಿನ ಫಿಲ್ಟರ್‌ನಂತೆ ಕಾರ್ಯನಿರ್ವಹಿಸುತ್ತವೆ (ಉದಾ ಇಂಟರ್ನೆಟ್) ನಂಬಲಾಗದ ಮತ್ತು ಸುರಕ್ಷಿತವಲ್ಲ ಎಂದು ಭಾವಿಸಲಾಗಿದೆ
- ಯಾವ ಮಾಹಿತಿ ಪ್ಯಾಕೆಟ್‌ಗಳನ್ನು ಅನುಮತಿಸಲಾಗಿದೆ ಮತ್ತು ನಿರ್ಬಂಧಿಸಲಾಗಿದೆ ಎಂಬುದನ್ನು ನಿಯಂತ್ರಿಸಲು ಫೈರ್‌ವಾಲ್ ಫಿಲ್ಟರ್ ಅನ್ನು ಮೃದುವಾಗಿ ಪ್ರೋಗ್ರಾಮ್ ಮಾಡಬಹುದು

Q1 7.ಆಂಟಿ-ವೈರಸ್ ಸಾಫ್ಟ್‌ವೇರ್ ಎಂದರೇನು?

- ಆಂಟಿ-ವೈರಸ್ ಸಾಫ್ಟ್‌ವೇರ್ ಫೈಲ್‌ಗಳನ್ನು ಸ್ಕ್ಯಾನ್ ಮಾಡಲು ಬಳಸುವ ಕಂಪ್ಯೂಟರ್ ಸಾಫ್ಟ್ ವೇರ್ ಆಗಿದೆ ದುರುದ್ದೇಶಪೂರಿತ ಸಾಫ್ಟ್‌ವೇರ್ (ಮಾಲ್‌ವೇರ್) ಗುರುತಿಸಿ ಮತ್ತು ತೊಡೆದುಹಾಕಲು

Q18. ಸೈಬರ್ ಭದ್ರತೆ ಮತ್ತು ಕ್ರಿಪ್ಟೋಗ್ರಫಿ ನಡುವಿನ ಸಂಬಂಧವೇನು?

- ಸೈಬರ್ ಭದ್ರತಾ ರಕ್ಷಣೆಗಳು ಬಲವಾದ ದೃಢೀಕರಣ ಮತ್ತು ಎನ್‌ಕ್ರಿಪ್ಶನ್ ಅನ್ನು ಆಧರಿಸಿವೆ ತಂತ್ರಗಳು (ಕ್ರಿಪ್ಟೋಗ್ರಫಿ ತಂತ್ರಗಳು)
- ಕ್ರಿಪ್ಟೋಗ್ರಫಿಯು ಸೈಬರ್ ಸುರಕ್ಷತೆಗೆ ಪ್ರಮುಖ ಸಕ್ರಿಯಗೊಳಿಸುವ ತಂತ್ರಜ್ಞಾನವಾಗಿದೆ
- ಸೈಬರ್ ಭದ್ರತೆಯನ್ನು ಕಾರ್ಯಗತಗೊಳಿಸಲು ಕ್ರಿಪ್ಟೋಗ್ರಫಿ ಸಹಾಯ ಮಾಡುತ್ತದೆ