ಡಿಸೆಂಬರ್ ೨೦೨೧ | DECEMBER 2021

ಸೈಬರ್ ವಾರ್ತಿಕಾ
CYBER VARTIKA

ಸೈಸೆಕ್ ಸೈಬರ್ ಸೆಕ್ಯುರಿಟಿ ಕರ್ನಾಟಕ
ಕೆ-ಟೆಕ್ ಉನ್ನತಜ್ಞಾನ ಕೇಂದ್ರ

CySecK Cyber Security Karnataka
K-Tech CoE for Cyber Security

ಮುನ್ನುಡಿ /Foreword

ನಲ್ಮೆಯ ಓದುಗರೆ,

2021 ಮುಗಿದು, 2022 ರ ಹೊಸ ವರ್ಷವನ್ನು ಬರಮಾಡಿಕೊಳ್ಳುವ ಈ ಹೊತ್ತಿನಲ್ಲಿ, ಕೋವಿಡ್‌ನ ಬಿಗಿಹಿಡಿತದಿಂದ ನಾವು ಇನ್ನೂ ಪೂರ್ತಿಯಾಗಿ ಬಿಡುಗಡೆ ಪಡೆದಿಲ್ಲ. ಹಾಗಾಗಿ, ಕೆಲಸದ ವಿಷಯವೇ ಆಗಿರಬಹುದು, ಶಾಲೆ ಇಲ್ಲವೇ ಬೇರೆ ದಿನನಿತ್ಯದ ಚಟುವಟಿಕೆಗಳೇ ಆಗಿರಬಹುದು, ನಮ್ಮ ಬದುಕಿನ ಬಹಳಷ್ಟು ವಿಷಯಗಳು ಇನ್ನೂ ಸೈಬರ್ ಜಗತ್ತನ್ನೇ ನೆಚ್ಚಿಕೊಂಡಿವೆ. ಸೈಬರ್ ಅಪರಾಧಿಗಳು ಕೂಡ ಜನರಿಗೆ ಮೋಸ ಮಾಡುವ ಅವಕಾಶಗಳಿಗಾಗಿ ಹುಡುಕುತ್ತಲೇ ಇದ್ದಾರೆ.

ಕಳೆದ ತಿಂಗಳು ದೊಡ್ಡದಾಗಿ ಸದ್ದು ಮಾಡಿದ ಸುದ್ದಿಯೆಂದರೆ log4j ತೊಂದರೆ. ಹಲವು ಸಾಫ್ಟ್‌ವೇರ್‌ಗಳು ಬಳಸುವ, ಪ್ರಮುಖವಾದ ಲೈಬ್ರರಿಗಳೆಂಬ ಪ್ರೋಗ್ರಾಮಿಂಗ್ ಕೋಡ್‌ಗಳಲ್ಲಿ, ಗಂಭೀರವಾದ ದೋಷಗಳು ಯಾವಾಗ ಬೇಕಾದರೂ ಕಾಣಿಸಿಕೊಳ್ಳಬಹುದು ಎಂದು ಈ log4j ತೊಂದರೆ ಮತ್ತೊಮ್ಮೆ ನೆನಪಿಸಿದೆ. ನಮ್ಮ ಸಾಫ್ಟ್‌ವೇರ್ ಅಭಿವೃದ್ಧಿ ಮತ್ತು ಸೈಬರ್ ಸುರಕ್ಷತೆಯ ತಿಳಿವನ್ನು ಹೆಚ್ಚಿಸುವುದರಲ್ಲಿ ಇನ್ನೂ ಸುಧಾರಣೆಯಾಗಬೇಕು ಎಂಬ ಅಗತ್ಯವನ್ನು ಕೂಡ ಈ ತೊಂದರೆ ತೋರಿಸಿಕೊಟ್ಟಿದೆ. ಬಹುತೇಕ ವಾಣಿಜ್ಯ ಬಳಕೆಯ ಸಾಫ್ಟ್‌ವೇರ್‌ಗಳು ದೋಷಮುಕ್ತವಾಗಿರಬೇಕೆಂದು ಎದುರುನೋಡುವುದು ಸಮಂಜಸವಲ್ಲ. ಆದ್ದರಿಂದಲೇ ಪ್ರಮುಖ ಸೈಬರ್ ಸುರಕ್ಷತೆ ವಿಷಯಗಳ ಬಗ್ಗೆ ಸಾಕಷ್ಟು ತಿಳಿವು ನಮಗೆ ಇರಬೇಕಾದದ್ದು ತುಂಬ ಮುಖ್ಯ. ಇಂತಹ ತಿಳಿವು ಇದ್ದರೆ, ಹೊಸದಾಗಿ ಬೆಳಕಿಗೆ ಬಂದ ಸಾಫ್ಟ್‌ವೇರ್ ದೋಷಗಳ ಗಂಭೀರತೆ ಮತ್ತು ತಾಂತ್ರಿಕ ರಚನೆಗಳನ್ನು ಬೇಗನೆ ಅರ್ಥಮಾಡಿಕೊಳ್ಳಲು ನಮಗೆ ತುಂಬ ನೆರವಾಗುತ್ತದೆ. ಆಗ, ನಾವು ಸೂಕ್ತವಾದ ಪರಿಹಾರಗಳನ್ನು ಕಂಡುಹಿಡಿಯಬಹುದು.

ಜಗತ್ತಿನಲ್ಲಿ ಆಗುತ್ತಿರುವ ಪ್ರಮುಖ ಸೈಬರ್ ಸುರಕ್ಷತೆ ಬೆಳವಣಿಗೆಗಳ ಬಗ್ಗೆ ಜನರಿಗೆ ತಿಳಿಸಿಕೊಡಬೇಕಾದ ಅಗತ್ಯವನ್ನು "ಸೈಬರ್ ವಾರ್ತಿಕಾ" ಪೂರೈಸುತ್ತದೆ ಎಂದು ನಾನು ನಂಬಿದ್ದೇನೆ. log4j ಹಾಗೂ ಬೇರೆ ಸೈಬರ್ ಸುರಕ್ಷತೆ ತೊಂದರೆಗಳ ಬಗ್ಗೆ ಇನ್ನಷ್ಟು ತಿಳಿಯಲು, ಈ ಸುದ್ದಿಪತ್ರಿಕೆಯಲ್ಲಿರುವ ತುಣುಕುಗಳು ನಿಮ್ಮನ್ನು ಹುರಿದುಂಬಿಸಲಿ ಎಂದು ನಾನು ಹಾರೈಸುತ್ತೇನೆ.

-- ವಿನೋದ್ ಗಣಪತಿ,
ಸಹ ಪ್ರಾಧ್ಯಾಪಕ, ಕಂಪ್ಯೂಟರ್ ವಿಜ್ಞಾನ ಮತ್ತು ಆಟೊಮೇಶನ್ ವಿಭಾಗ,
ಭಾರತೀಯ ವಿಜ್ಞಾನ ಸಂಸ್ಥೆ, ಬೆಂಗಳೂರು

Dear Readers,

As we call an end to 2021 and start 2022, we are still very much in the throes of uncertainty surrounding Covid. As a result, many aspects of our lives continue to be dependent on the cyber world, be it work-related, school-related, or other daily activities. Cyber security criminals are also on the continuous lookout for opportunities to defraud people.

The major cyber security news this past month was the log4j vulnerability. This vulnerability was a reminder that serious flaws continue to lurk in important libraries used by many software packages, and underscores the need to continuously improve our software development practices and our cyber security awareness. It is not realistic to expect most commercial software to be completely free of software vulnerabilities. This is precisely why it is important for us to have sufficient awareness of major cyber security concepts. Such awareness goes a long way in helping us quickly understand the seriousness of and technical underpinnings of a newly-discovered vulnerability, so that we can devise suitable countermeasures.

It is my hope that 'Cyber Vartika' serves this important need to keep the community informed about major cyber security happenings around the world. I hope that the tidbits in this newsletter inspire you to learn more about log4j and other cyber security vulnerabilities listed herein.

-- Vinod Ganapathy,
Associate Professor, Department of Computer Science and Automation,
Indian Institute of Science Bangalore.

ಪ್ರಮುಖ ಸೈಬರ್ ಸುದ್ದಿ

ಕರ್ನಾಟಕದಲ್ಲಿ ಸೈಬರ್ ಅಪರಾಧದ ಬಗ್ಗೆ ದೂರು ನೀಡಲು 112 ಕ್ಕೆ ಕರೆಮಾಡಿ.

ಕರ್ನಾಟಕದ ಎಲ್ಲಾ ಜಿಲ್ಲೆಗಳ ನಾಗರಿಕರು, 2022 ರ ಜನವರಿ ಕೊನೆಯ ಹೊತ್ತಿಗೆ, ದಿನದ 24 ಗಂಟೆಯೂ 112 ನಂಬರ್‌ಗೆ ಕರೆಮಾಡಿ ಸೈಬರ್ ಅಪರಾಧದ ದೂರು ಸಲ್ಲಿಸಬಹುದು.

2020 ರ ಡಿಸೆಂಬರ್‌ನಿಂದಲೇ ಬೆಂಗಳೂರು ಪೊಲೀಸ್ ಇಲಾಖೆಯು, 112 ನಂಬರ್‌ನಲ್ಲಿ ಸೈಬರ್ ಅಪರಾಧದ ದೂರುಗಳನ್ನು ಪಡೆಯುತ್ತಿದೆ. ಕಳೆದ 11 ತಿಂಗಳಲ್ಲಿ, ನಗರ ಪೊಲೀಸ್ ಇಲಾಖೆಯು, 7,000 ಮಂದಿಗೆ ಸೇರಿದ ಅಂದಾಜು 70 ಕೋಟಿ ರೂಪಾಯಿಗಳ ವರ್ಗಾವಣೆಯನ್ನು ತಪ್ಪಿಸಿದೆ.

ಕೇಂದ್ರ ಸಚಿವಾಲಯದ ಅಧಿಕಾರಿಗಳನ್ನು ಗುರಿಯಾಗಿಸಿ ಚುರುಕುಗೊಂಡ ಫಿಶಿಂಗ್ ದಾಳಿಗಳು

ಹಲವಾರು ಕೇಂದ್ರ ಸಚಿವಾಲಯಗಳ ಉದ್ಯೋಗಿಗಳಿಗೆ ಸ್ಫೋಟಕ ಹೇಳಿಕೆಯಿರುವ ಗುಟ್ಟಿನ ಇಮೇಲ್ ಬಂದಿರುವುದಾಗಿ ಇಂಡಿಯನ್ ಎಕ್ಸ್‌ಪ್ರೆಸ್ ಪತ್ರಿಕೆ ವರದಿ ಮಾಡಿದೆ.

ತನ್ನ ನೆಟ್‌ವರ್ಕ್‌ಗೆ ಅನಧಿಕೃತ ಪ್ರವೇಶ ಆಗಿರುವುದನ್ನು ಒಪ್ಪಿಕೊಂಡ ಪ್ಯಾನಸೋನಿಕ್, ಸೈಬರ್ ದಾಳಿ ವಿಚಾರಣೆ ನಡೆಯುತ್ತಿದೆ

ಜಪಾನಿನ ಗ್ರಾಹಕ ಎಲೆಕ್ಟ್ರಾನಿಕ್ಸ್ ಕಂಪನಿಯಾದ ಪ್ಯಾನಸೋನಿಕ್, ತನ್ನ ನೆಟ್‌ವರ್ಕ್‌ನೊಳಗೆ ನವಂಬರ್ 11 ರಂದು ಯಾರೋ ಹೊರಗಿನವರು ಮೋಸದಿಂದ ನುಸುಳಿದ್ದು ನಿಜ ಎಂದು ಖಚಿತಪಡಿಸಿದೆ.

ಕಂಪನಿಯು ಹೆಚ್ಚುವರಿ ಮಾಹಿತಿ ನೀಡದಿದ್ದರೂ, ಜಪಾನಿನ ಸುದ್ದಿ ಸಂಸ್ಥೆಗಳಾದ ಮೈನೀಚಿ ಮತ್ತು ಎನ್‌ಎಚ್‌ಕೆ, ನುಸಳುಕೋರರು ಜೂನ್ 22 ರಿಂದಲೇ ಪ್ರಯತ್ನಿಸುತ್ತಿದ್ದು, ನವಂಬರ್ 3 ರಂದು ನೆಟ್‌ವರ್ಕ್ ಒಳನುಗ್ಗಿದ್ದಾರೆ ಎಂದು ಹೇಳಿವೆ.

ಸೋರಿಕೆಯ ಬಗ್ಗೆ ಹೆಚ್ಚಿನ ಮಾಹಿತಿ ಕಲೆಹಾಕಲು ಹಾಗೂ ತನ್ನ ಬಳಕೆದಾರರ ವೈಯಕ್ತಿಕ ಮಾಹಿತಿ ಮತ್ತು/ಇಲ್ಲವೇ ಸಾಮಾಜಿಕ ಮೂಲಸೌಕರ್ಯಕ್ಕೆ ಸಂಬಂಧಿಸಿದ ಗುಟ್ಟಾದ ಡೇಟಾದ ಮೇಲೆ ಪರಿಣಾಮ ಉಂಟಾಗಿದೆಯೇ ಎಂದು ನೋಡಲು, ಹೊರಗಿನ ಪರಿಣತ ಸಂಸ್ಥೆಯೊಂದಿಗೆ ಕೆಲಸ ಮಾಡುತ್ತಿರುವುದಾಗಿ ಪ್ಯಾನಸೋನಿಕ್ ಹೇಳಿದೆ.

2021 ರ ಜಾಗತಿಕ ಡೇಟಾ ಕಳ್ಳತನದಲ್ಲಿ ಭಾರತಕ್ಕೆ ಮೂರನೇ ಸ್ಥಾನ

ಸರ್ಫ್‌ಶಾರ್ಕ್ ಎಂಬ ಸೈಬರ್ ಸುರಕ್ಷತೆ ಕಂಪನಿ ನಡೆಸಿದ ಸಂಶೋಧನೆಯ ಪ್ರಕಾರ, ನವೆಂಬರ್ 2021 ರ ವರೆಗೆ ಸುಮಾರು 8.66 ಕೋಟಿ ಭಾರತೀಯ ಬಳಕೆದಾರರ ಡೇಟಾ ಕಳ್ಳತನವಾಗುವುದರೊಂದಿಗೆ, ಜಗತ್ತಿನ ಡೇಟಾ ಕಳ್ಳತನದಲ್ಲಿ ಭಾರತವು ಮೂರನೇ ಸ್ಥಾನದಲ್ಲಿದೆ. ಈ ವರ್ಷದಲ್ಲಿ, ಅತಿ ಹೆಚ್ಚು ಡೇಟಾ ಸೋರಿಕೆಗೆ ಒಳಗಾದದ್ದು COMB, ಕ್ಲಬ್‌ಹೌಸ್, ಫೇಸ್‌ಬುಕ್ ಮತ್ತು ರೇಚಾಟ್ ಎಂದು ಸಂಶೋಧನೆ ಹೇಳುತ್ತಿದೆ.

ಹಿಂದಿನ ವರ್ಷಕ್ಕೆ ಹೋಲಿಸಿದಾಗ, ಸೋರಿಕೆಯ ಬಿಸಿ ತಟ್ಟಿದ ಖಾತೆಗಳ ಎಣಿಕೆ ಭಾರತದಲ್ಲಿ 351.6 % ನಷ್ಟು ಹೆಚ್ಚಾಗಿತ್ತು. 2020 ರಲ್ಲಿ ಹೆಚ್ಚುಕಡಿಮೆ 1.92 ಕೋಟಿ ಭಾರತೀಯ ಬಳಕೆದಾರರ ಡೇಟಾ ಕಳ್ಳತನವಾಗಿತ್ತು. “ಡೇಟಾ ಕಳ್ಳತನ ಪ್ರಕರಣಗಳು, ಕಳೆದ ವರ್ಷಕ್ಕಿಂತ ಈ ವರ್ಷ ತುಸು ಹೆಚ್ಚಾಗಿವೆ,” ಎಂದು ಸರ್ಫ್‌ಶಾರ್ಕ್ ಹೇಳಿದೆ.

ಪ್ರಮುಖ ಸೈಬರ್ ಸುದ್ದಿ

10 ತಿಂಗಳಲ್ಲಿ ಸೈಬರ್ ದಾಳಿಗೆ ತುತ್ತಾದ 26,000 ಭಾರತೀಯ ವೆಬ್‌ಸೈಟ್‌ಗಳು

ಎಲೆಕ್ಟ್ರಾನಿಕ್ಸ್ ಮತ್ತು ಐಟಿ ರಾಜ್ಯ ಸಚಿವ ರಾಜೀವ್ ಚಂದ್ರಶೇಖರ್, "CERT-IN ವರದಿ ಹೇಳುವಂತೆ, 17,560, 24,768, 26,121, ಮತ್ತು 25,870 ಭಾರತೀಯ ವೆಬ್‌ಸೈಟ್‌ಗಳು ಕ್ರಮವಾಗಿ 2018, 2019, 2020 ಮತ್ತು 2021 (ಅಕ್ಟೋಬರ್‌ವರೆಗೆ) ರಲ್ಲಿ ದಾಳಿಗೆ ತುತ್ತಾಗಿವೆ." ಎಂದು ಹೇಳಿದ್ದಾರೆ. ಭವಿಷ್ಯದಲ್ಲಿ ಸೈಬರ್ ದಾಳಿಗಳನ್ನು ತಡೆಯುವ ಸಲುವಾಗಿ, ಸೈಬರ್ ಸುರಕ್ಷತೆಯ ನಿಲುವನ್ನು ಸುಧಾರಿಸಲು ಸರ್ಕಾರ ಹಲವು ಕ್ರಮಗಳನ್ನು ಕೈಗೊಂಡಿದೆ ಎಂದು ಕೂಡ ಅವರು ನುಡಿದಿದ್ದಾರೆ.

ಮೈಕ್ರೋಸಾಫ್ಟ್ ಆಪರೇಟಿಂಗ್ ಸಿಸ್ಟಮ್‌ನ ಕೊರತೆಯನ್ನು ಗುರಿಯಾಗಿಸಿ ಹೊಸ ದಾಳಿ

MSHTML ಮೇಲೆ ಪರಿಣಾಮ ಬೀರುತ್ತಿದ್ದ ಆಪರೇಟಿಂಗ್ ಸಿಸ್ಟಮ್‌ನ ಕೊರತೆಯನ್ನು ಕಂಡುಹಿಡಿದು, ಅದನ್ನು ನೀಗಿಸಲು ಮೈಕ್ರೋಸಾಫ್ಟ್ ಅಪ್‌ಡೇಟ್ ಅನ್ನು ಬಿಡುಗಡೆ ಮಾಡಿತ್ತು. ಆದರೆ, ಮೈಕ್ರೋಸಾಫ್ಟ್‌ನ ಅಪ್‌ಡೇಟ್ ಅನ್ನು ತಪ್ಪಿಸಿಕೊಂಡು, Formbook ಎಂಬ ಅಪಾಯಕಾರಿ ಸಾಫ್ಟ್‌ವೇರ್ ಅನ್ನು ಹರಡಲು ದಾಳಿಕೋರರು ನೋಡಿದರು. ಅವರ ಈ ಪ್ರಯತ್ನ ಹೆಚ್ಚು ದಿನ ಉಳಿಯಲಿಲ್ಲ.

"ತಮಗೆ ಗೊತ್ತಿಲ್ಲದ ವ್ಯಕ್ತಿಗಳು ಇಲ್ಲವೇ ಸಂಸ್ಥೆಗಳಿಂದ ಬಂದ, ವಿಚಿತ್ರವಾದ ಇಲ್ಲವೇ ಗೊತ್ತಿಲ್ಲದ ಫೈಲ್ ಫಾರ್ಮಾಟ್‌ನಲ್ಲಿರುವ ಇಮೇಲ್ ಕಡತಗಳ ಬಗ್ಗೆ ತುಂಬ ಎಚ್ಚರಿಕೆಯಿಂದಿರಬೇಕು ಎಂದು ಕೆಲಸಗಾರರಲ್ಲಿ ಅರಿವು ಮೂಡಿಸುವುದು ಮತ್ತು ಅವರಿಗೆ ನೆನಪಿಸುವುದು ತುಂಬ ಮುಖ್ಯ. ಬಳಕೆದಾರರನ್ನು ಕಾಪಾಡಲು, ಈ ಕಳವಳಗಳ ಬಗ್ಗೆ ನಾವು ಮರುನೋಟ ಮಾಡುತ್ತಿದ್ದು, ಬೇಕಾದ ಸರಿಯಾದ ಕ್ರಮಗಳನ್ನು ತೆಗೆದುಕೊಳ್ಳುತ್ತೇವೆ." ಎಂದು ಮೈಕ್ರೋಸಾಫ್ಟ್‌ನ ವಕ್ತಾರರು ಹೇಳಿಕೆ ನೀಡಿದ್ದಾರೆ.

ವಿದ್ಯಾರ್ಥಿನಿಯರಿಗೆ ಡಿಜಿಟಲ್ ಸಾಕ್ಷರತೆ ಒದಗಿಸುವ ಗುರಿ ಇಟ್ಟುಕೊಂಡ NCW

ಫೇಸ್‌ಬುಕ್ ಮತ್ತು ಸೈಬರ್ ಪೀಸ್ ಫೌಂಡೇಶನ್ ಸಂಸ್ಥೆಗಳ ಜೊತೆಗೂಡಿ ಜಾರಿ ಮಾಡಲಾದ 'We Think Digital' ಅಭಿಯಾನದ ಅಂಗವಾಗಿ, ರಾಷ್ಟ್ರೀಯ ಮಹಿಳಾ ಆಯೋಗವು (NCW) ಇತ್ತೀಚೆಗೆ ಸೈಬರ್ ಸುರಕ್ಷತೆ ಕುರಿತಾದ ಆನ್‌ಲೈನ್ ಕಲಿಕಾ ಕೇಂದ್ರವನ್ನು ಹೊರತಂದಿದೆ.

ಈ ತೊಡಗಿಕೆಯು, ಕೆಚ್ಚನ್ನು ಹೆಚ್ಚಿಸುವ ಹಾಗೂ ಆದಷ್ಟೂ ಸಮರ್ಥವಾದ ಬಗೆಯಲ್ಲಿ ಸೈಬರ್ ಅಪರಾಧವನ್ನು ಎದುರಿಸುವ ಅಳವನ್ನು ಹೆಚ್ಚಿಸುವ ಗುರಿ ಹೊಂದಿದೆ. ಡೇಟಾ ಗೌಪ್ಯತೆ, ಸಾಮಾಜಿಕ ಜಾಲತಾಣ ಸುರಕ್ಷತೆ, ಸೈಬರ್ ನಡವಳಿಕೆ, ಡಿಜಿಟಲ್ ಆರೋಗ್ಯ, ಸೈಬರ್ ಕಾನೂನು ಮತ್ತು ಸೈಬರ್ ಅಪರಾಧ ವಿಷಯಗಳ ಬಗ್ಗೆ ಇಲ್ಲಿ ಕಲಿಯಬಹುದು. ಇಡೀ ದೇಶದ ಕಾಲೇಜು ವಿದ್ಯಾರ್ಥಿನಿಯರು ಹುರುಪಿನಿಂದ ಈ ತೊಡಗಿಕೆಯಲ್ಲಿ ಪಾಲ್ಗೊಳ್ಳುತ್ತಿದ್ದಾರೆ.

ಪ್ರಮುಖ ಸೈಬರ್ ಸುದ್ದಿ

ಆನ್‌ಲೈನ್ ಮೋಸಗಳು

ಆನ್‌ಲೈನ್ ಮೋಸದ ಬಲೆಯಲ್ಲಿ ಬಿದ್ದ ಅಜ್‌ಮೀರ್‌ನ 2 ಮಂದಿ

ಮ್ಯಾಟ್ರಿಮೋನಿಯಲ್ ವೆಬ್‌ಸೈಟ್ ಮೋಸದಲ್ಲಿ 9.25 ಲಕ್ಷ ಕಳೆದುಕೊಂಡ ಟೆಕಿ

ಮ್ಯಾಟ್ರಿಮೋನಿಯಲ್ ವೆಬ್‌ಸೈಟ್‌ನಲ್ಲಿ ಭೇಟಿಯಾದ ಹೆಂಗಸಿನಿಂದ ಮೋಸಕ್ಕೊಳಗಾದ ಮದುಮಗ

5 ಲಕ್ಷಕ್ಕೂ ಮೀರಿದ ಆನ್‌ಲೈನ್ ಮೋಸಗಳಿಗೆ ಒಳಗಾದ 26 ಮಂದಿ

ಆನ್‌ಲೈನ್ ಮೋಸಗಾರರ ಬಲೆಗೆ ಬಿದ್ದ ಡಾಕ್ಟರ್

ಮಾಜಿ ಭಾರತೀಯ ಕ್ರಿಕೆಟ್ ಆಟಗಾರ ವಿನೋದ್ ಕಾಂಬ್ಳಿಗೆ 1.14 ಲಕ್ಷ ಮೋಸ

ಮಂಗಳೂರು: ಸೈಬರ್ ಮೋಸದಲ್ಲಿ 2.94 ಲಕ್ಷ ಕಳೆದುಕೊಂಡ ಹೆಂಗಸು

ಸೈಬರ್ ಮೋಸದಲ್ಲಿ 8 ಲಕ್ಷ ಕಳೆದುಕೊಂಡ ಹೆಂಗಸು

ಸೈಬರ್ ಮೋಸ: ವಿದ್ಯಾರ್ಥಿಗಳಿಂದ ಹಣ ದೋಚುತ್ತಿದ್ದ ರಾಜಸ್ಥಾನ ಮೂಲದ 3 ಮಂದಿಯ ಸೆರೆ

2.5 ಲಕ್ಷ ಸೈಬರ್ ಮೋಸಕ್ಕೆ ಒಳಗಾದ ಇಂಜಿನಿಯರಿಂಗ್ ವಿದ್ಯಾರ್ಥಿ

ವಿದ್ಯುತ್ ಬಿಲ್ ಮೋಸ: KSEB ಬಳಕೆದಾರರಿಂದ 2 ಲಕ್ಷ ದೋಚಿದ ಉತ್ತರ ಪ್ರದೇಶದ ಕಳ್ಳರ ಕೂಟ

12 ಸೈಬರ್ ಅಪರಾಧಿಗಳು ಬೆಂಗಳೂರಿನಲ್ಲಿ ಸೆರೆ

Top Cyber News

Dial 112 to report cybercrime in Karnataka

Citizens from all districts of Karnataka will be able to report cybercrime anytime of the day (24/7) by the end of January 2022 by dialling 112.
Bengaluru police has been receiving cybercrime complaints on 112 since December 2020. The city police have halted the transfer of approximately 70 crore belonging to 7,000 people in the last 11 months.

Phishing attacks on central ministry officials get sharper, targeted

Indian Express reports that several employees of various central ministries received mysterious emails with sensational claims.

Panasonic acknowledges unauthorised access to its network, probing cyber attack

Panasonic, a Japanese consumer electronics company, confirmed that a third party fraudulently accessed its network on November 11.
While the firm gave no additional information, Japanese outlets Mainichi and NHK said that the hack began on June 22 and ended on November 3.
Panasonic said it is working with a specialist third-party organisation to examine the leak and determine whether it impacted customers' personal information and/or sensitive data related to social infrastructure.

India ranks third in global data breaches in 2021

According to research conducted by a cybersecurity company Surfshark, India ranks third in the world in terms of data breaches, with 86.63 million Indian customers breached till November 2021. COMB, Clubhouse, Facebook, and Raychat were among the biggest data breaches this year, according to the research.
When compared to the previous year, India had a 351.6% increase in affected accounts. The data of approximately 19.18 million Indian users was breached in 2020. "In terms of data breach cases, this year was marginally worse than last year," it claimed.

Top Cyber News

‘Cyberattacks hit 26,000 Indian sites in 10 months’

Minister of State for Electronics and IT Rajeev Chandrasekhar said: "CERT-In has reported that a total of 17,560, 24,768, 26,121, and 25,870 Indian websites were hacked during the years 2018, 2019, 2020, and 2021 (up to October), respectively." He added that the government has taken various measures to enhance the cybersecurity posture and prevent cyberattacks in the coming future.

New Exploit seen in Microsoft

With the purpose of transmitting Formbook malware, a short-lived phishing effort was noticed that took advantage of an unique exploit that evaded a patch put in place by Microsoft to solve a remote code execution vulnerability affecting the MSHTML component.
"It's critical to educate and remind staff to be wary of emailed documents, especially when they arrive in strange or unknown compressed file formats from persons or organizations they don't know”. "We are reviewing these concerns and will take appropriate action as needed to help keep customers protected," a Microsoft spokeswoman stated.

NCW aims to provide digital literacy to girl students

As part of the 'We Think Digital' campaign, which is implemented in conjunction with Facebook and the Cyber Peace Foundation, the National Commission for Women (NCW) has recently launched an online resource centre on cyber safety.
The initiative aims to increase resilience and the ability to combat cybercrime in the most efficient manner possible. Data Privacy, Social Media Safety, Cyber Ethics, Digital Wellbeing, Cyber Laws, and Cyber Crimes are among the topics covered. College going girls from all over the country are actively participating in the initiative.

Top Cyber News

ONLINE FRAUDS

2 people fall prey to online fraud in Ajmer

Techie duped of Rs 9.25L in matrimonial site fraud

Prospective groom duped by woman he met on matrimonial site

26 fell victim to online frauds of over Rs 5L

Doctor falls prey to online fraudsters

Former Indian cricketer Vinod Kambli duped of Rs 1.14 lakh

Mangaluru: Woman cheated of Rs 2.94 lakh in cyber fraud

Woman loses around Rs 8 lakh in cyber fraud

Cyber fraud: 3 Rajasthan natives held for swindling money from students

Engineering student duped of Rs 2.50 lakh in cyber fraud

Electricity bill fraud: UP gang embezzles Rs 2 lakh from KSEB consumers

12 cyber criminals arrested in Bengaluru

ಸೈಸೆಕ್ ಜಾಗೃತಿ ಭಂಡಾರ

Log4Shell™

ದೌರ್ಬಲ್ಯ

ಸೈಸೆಕ್
ಸೈಬರ್ ಸೆಕ್ಯುರಿಟಿ ಕರ್ನಾಟಕ
ಕೆ-ಟೆಕ್ ಉನ್ನತಜ್ಞಾನ ಕೇಂದ್ರ

Log4Shell ಎಂದರೇನು?

ಎಲ್ಲೆಡೆ ಬಳಸಲಾಗುವ Log4j ಸಾಫ್ಟ್‌ವೇರ್‌ನಲ್ಲಿ ಭದ್ರತೆಯ ದೌರ್ಬಲ್ಯ ವಿರುವುದನ್ನು ಅಲಿಬಾಬ ಎಂಬ ಚೀನಾದ ಕಂಪನಿಯ ಭದ್ರತೆ ತಂಡವು ಗಮನಿಸಿ, 2021 ರ ಡಿಸೆಂಬರ್ 5 ರಂದು ಈ ವಿಷಯ ಬಯಲುಮಾಡಿತು. ಈ ತೊಂದರೆಯನ್ನು ಬೇಗನೆ ಸರಿಪಡಿಸಲು ಜಗತ್ತಿನ ಎಲ್ಲ ಐಟಿ ತಂಡಗಳು ಹಗಲಿರುಳು ದುಡಿಯುತ್ತಿವೆ.
ಈ ತೊಂದರೆಯ
ಹೆಸರೇ Log4Shell.

LOG4J

Log4j ಎಂದರೇನು?

Log4j ಎಂಬುದು ಜಾವ ಎಂಬ ಪ್ರೋಗ್ರಾಮಿಂಗ್ ನುಡಿಯಲ್ಲಿ ಬರೆದ, ಹೆಸರುವಾಸಿಯಾದ ಓಪನ್-ಸೋರ್ಸ್
(ಅಂದರೆ ಯಾರು ಬೇಕಾದರೂ ತಿದ್ದಿ, ಎಲ್ಲರೊಡನೆ ಹಂಚಿಕೊಳ್ಳಬಹುದಾದ ಸಾಫ್ಟ್‌ವೇರ್) ಸಾಫ್ಟ್‌ವೇರ್ ಆಗಿದ್ದು,ಇದಕ್ಕೆ ಅಪಾಚೆ ಸಾಫ್ಟ್‌ವೇರ್ ಫೌಂಡೇಶನ್ ಸಂಸ್ಥೆಯ ಬೆಂಬಲವಿದೆ. ಇದನ್ನು ಎಲ್ಲೆಡೆ ಬಳಸಲಾಗುತ್ತದೆ. ಏಕೆಂದರೆ ಇದರಿಂದಾಗಿ, ಸಾಫ್ಟ್‌ವೇರ್ ಮಾಡುವವರು ಬೇಗನೆ, ನಂಬತಕ್ಕ ಮತ್ತು ಸರಳವಾಗಿ ತಿದ್ದಬಹುದಾದ ಬಗೆಯಲ್ಲಿ ಅಪ್ಲಿಕೇಶನ್ ಲಾಗ್‌ಗಳನ್ನು
ಸುಲಭವಾಗಿ ರಚಿಸಬಹುದು.

ಇದರ ಬಗ್ಗೆ ಏಕೆ ಇಷ್ಟೊಂದು ಕಳವಳ?

ಮೂರು ಕಾರಣಗಳಿಗಾಗಿ!

1. *Log4j* ಅನ್ನು ಎಲ್ಲೆಡೆ ಬಳಸಲಾಗುತ್ತಿದೆ. ನಮ್ಮಲ್ಲಿರುವ ಬಹುಪಾಲು ಐಟಿ ಸಿಸ್ಟಮ್‌ಗಳು *Log4j* ಬಳಸುತ್ತಿರಬಹುದು. ನಿಮಗೆ ಅದು ಗೊತ್ತಿಲ್ಲದಿರಬಹುದು. ಏಕೆಂದರೆ ನೀವು ಅದನ್ನು ನೇರವಾಗಿ ಬಳಸದಿದ್ದರೂ, ನಿಮ್ಮ ಕಂಪ್ಯೂಟರ್‌ಗಳಲ್ಲಿ ಇನ್‌ಸ್ಟಾಲ್ ಆಗಿರುವ ಕೆಲವು ಅಪ್ಲಿಕೇಶನ್‌ಗಳು ಸರಿಯಾಗಿ ಕೆಲಸ ಮಾಡಲು ಅದನ್ನು ಹಿನ್ನೆಲೆಯಲ್ಲಿ ಬಳಸುತ್ತಿರಬಹುದು.
2. Log4j ಅನ್ನು ಮೋಸದಿಂದ ಬಳಸಿಕೊಳ್ಳುವುದು ಸುಲಭ. ವಿಶೇಷವಾಗಿ ರೂಪಿಸಲಾದ ಒಂದು ಇನ್‌ಪುಟ್ ಸ್ಟ್ರಿಂಗ್ ಅನ್ನು ಕಳುಹಿಸಿದರೆ ಸಾಕು. ಇಂತಹ ಮೋಸದ ಬಳಕೆಗಳು ಈಗಾಗಲೇ ಹೆಚ್ಚಾಗಿರುವುದು ತಿಳಿದುಬಂದಿದೆ.
3. ಇಂತಹ ಮೋಸದ ಬಳಕೆಯಿಂದ ತುಂಬ ಕೆಡುಕಾಗಬಹುದು. ಇದರ ಮೂಲಕ, ದಾಳಿಕೋರರು ದೂರದಿಂದಲೇ ಸಿಸ್ಟಮ್ ಅನ್ನು ಪೂರ್ತಿಯಾಗಿ ತಮ್ಮ ಹಿಡಿತಕ್ಕೆ ತೆಗೆದುಕೊಳ್ಳಬಹುದು.

ಬಿರುಗಾಳಿಯಂತೆ ಬಂದೆರಗಿದ ಈ ತೊಂದರೆಯ ಸರಿಪಡಿಕೆಗಾಗಿ, ಭದ್ರತೆ ಮತ್ತು ಐಟಿ ವೃತ್ತಿಪರರು ಈಗ ಹಗಲಿರುಳು ಕೆಲಸ ಮಾಡುತ್ತಿದ್ದಾರೆ.

ಸಾಫ್ಟ್‌ವೇರ್ ಮಾಡುವವರು ಇದನ್ನು ಏಕೆ ಬಳಸುತ್ತಾರೆ?

ಲಾಗ್ ಎಂದರೆ ನಾವು ಬರೆದಿಡುವ ಒಂದು ಡೈರಿಯಂತೆ. ಅಪ್ಲಿಕೇಶನ್‌ಗಳ ಚಟುವಟಿಕೆಗಳನ್ನು ದಾಖಲಿಸಲು ಇದನ್ನು ಬಳಸಲಾಗುತ್ತದೆ. ಉದಾಹರಣೆಗೆ, ತೊಂದರೆಗಳ ಬಗೆಹರಿಕೆಯಂತಹ ಉಪಯೋಗಗಳಿಗಾಗಿ, ಬೇಕಿದ್ದರೆ ಇದನ್ನು ಆಮೇಲೆ ಬಳಸಿಕೊಳ್ಳಬಹುದು. ಆದ್ದರಿಂದ ಅಪ್ಲಿಕೇಶನ್‌ನ ಚಟುವಟಿಕೆಗಳನ್ನು ಲಾಗ್ ಮಾಡುವುದು ಒಳ್ಳೆಯ ವಾಡಿಕೆ. ಯಾವುದನ್ನೆಲ್ಲ ಲಾಗ್ ಮಾಡಬೇಕು ಎಂಬ ಏರ್ಪಾಡು ಮಾಡಲು Log4j ನೆರವಾಗುತ್ತದೆ.

ಈ ತೊಂದರೆಯನ್ನು ಸರಿಪಡಿಸುವುದು ಹೇಗೆ?

ಈ ಭದ್ರತೆಯ ದೌರ್ಬಲ್ಯವನ್ನು ಸರಿಪಡಿಸಲಾಗಿರುವ ಹೊಸ ಆವೃತ್ತಿಯಾದ Log4j 2.17.0 ಈಗ ದೊರೆಯುತ್ತಿದೆ.

1010110101101011010110101
0101001010010100101001010
1010110101101011010110101

ಹಾಗಿದ್ದರೆ, ಇದರ ಬಗ್ಗೆ ಇನ್ನೂ ಕಳವಳ ಯಾಕೆ?

ಹಿಂದೆ ನಾವು ಕಂಡಂತೆ, ಇಷ್ಟು ದೊಡ್ಡ ಮಟ್ಟದಲ್ಲಿ ಸಾಫ್ಟ್‌ವೇರ್ ಅಪ್‌ಗ್ರೇಡ್ ಮಾಡಲು ಹಲವು ತಿಂಗಳುಗಳೇ ಹಿಡಿಯಬಹುದು. ಯಾವ ಸಿಸ್ಟಮ್‌ಗಳನ್ನು ಅಪ್‌ಗ್ರೇಡ್ ಮಾಡಬೇಕು ಎಂಬ ಪೂರ್ತಿ ಪಟ್ಟಿಯೇ ಐಟಿ ತಂಡದ ಬಳಿ ಇಲ್ಲದಿರಬಹುದು.
ಇದು, ಸಿಸ್ಟಮ್‌ಗಳನ್ನು ತಮ್ಮ ಹಿಡಿತಕ್ಕೆ ತೆಗೆದುಕೊಳ್ಳಲು, ದಾಳಿಕೋರರಿಗೆ ಬಹಳಷ್ಟು ಸಮಯ ನೀಡುತ್ತದೆ.

ಜೀರೋ-ಡೇ ವಲ್ನರಬಿಲಿಟಿ (zero-day vulnerability) ಎಂದರೇನು?

ಇನ್ನೂ ಸರಿಪಡಿಸಲಾಗದ ಭದ್ರತೆಯ ತೊಂದರೆಯನ್ನು ಜೀರೋ-ಡೇ ವಲ್ನರಬಿಲಿಟಿ ಎಂದು ಕರೆಯುತ್ತಾರೆ.
ಈ ತೊಂದರೆಯನ್ನು ಈಗ ಹೊಸ ಆವೃತ್ತಿಯಲ್ಲಿ ಸರಿಪಡಿಸಲಾಗಿದೆ.
ಹಾಗಾಗಿ ಈಗ ಇದು ಜೀರೋ-ಡೇ ವಲ್ನರಬಿಲಿಟಿ ಅಲ್ಲ.

ನಾನು ಈ ವಿಷಯದಲ್ಲಿ ಏನು ಮಾಡಬೇಕು?

ನಿಮ್ಮ ಐಟಿ ಸಿಸ್ಟಮ್‌ಗಳ ನಿರ್ವಹಣೆ ನಿಮ್ಮ ಹೊಣೆಯಾಗಿದ್ದರೆ, ಅವು Log4j ಬಳಸುತ್ತಿವೆಯೇ ಇಲ್ಲವೇ ಎಂದು ನೋಡಿ. ಅವು Log4j ಬಳಸುತ್ತಿದ್ದರೆ, ಕೂಡಲೇ ಅಪ್‌ಗ್ರೇಡ್ ಮಾಡಿ. ಜೊತೆಗೆ, ನಿಮಗೆ ಸಾಫ್ಟ್‌ವೇರ್ ಒದಗಿಸುವವರಿಗೂ ಕೂಡ (ಉದಾ: SaaS) Log4j ತೊಂದರೆಯ ಬಿಸಿ ತಟ್ಟಿದೆಯೇ ಎಂದು ಅವರನ್ನು ಕೇಳಿ ನೋಡಿ.
ಅವರು ಹೌದು ಎಂದರೆ, ಅದರ ಸರಿಪಡಿಕೆಗೆ ಏನು ಯೋಜನೆ ಹಾಕಿದ್ದಾರೆ ಎಂದು ಕೂಡ ಕೇಳಿ ತಿಳಿಯಿರಿ. ತೊಂದರೆ ಬಗೆಹರಿಯುವವರೆಗೂ, ಅವರ ಸಿಸ್ಟಮ್ ಬಳಸುವುದನ್ನು ನಿಲ್ಲಿಸುವ ಆಯ್ಕೆ ನಿಮಗಿದೆ.

ಸಾಮಾನ್ಯ ಕಂಪ್ಯೂಟರ್ ಮತ್ತು ಮೊಬೈಲ್ ಫೋನ್‌ಗಳಂತಹ ಐಟಿ ಸಾಧನಗಳನ್ನು ಬಳಸುವ ಸಾಮಾನ್ಯ ಬಳಕೆದಾರ ನೀವಾಗಿದ್ದರೆ, ಈ ತೊಂದರೆ ನೇರವಾಗಿ ನಿಮ್ಮನ್ನು ಕಾಡದೆ ಇರಬಹುದು.
ಆದರೆ, ಎಂದಿನಂತಿಲ್ಲದ, ಸಂದೇಹ ತರಿಸುವ ಚಟುವಟಿಕೆ ನಿಮ್ಮ ಗಮನಕ್ಕೆ ಬಂದರೆ, ಕೂಡಲೇ ಬಳಕೆದಾರರ ನೆರವು ತಂಡಕ್ಕೆ ತಿಳಿಸಿ.

Log4Shell™ VULNERABILITY

CySecK Cyber Security Karnataka

What is Log4Shell?

A security vulnerability in the widely used Log4j software was noticed by Chinese company Alibaba's security team and disclosed on 05-Dec-2021.
Now IT teams around the world are dashing to fix this issue.
This issue is called *Log4Shell*.

LOG4J

What is Log4j?

Log4j is a popular open-source software written in Java, and supported by The Apache Software Foundation. It is widely used because it makes it easy for developers to create application logs in a fast, reliable and flexible way

Why is it a big deal?

For three reasons!

1. Log4j is widely used. Probably most of the IT systems we have would be using Log4j. You may not even be aware of it, since even if you have not used it directly, some application you have deployed could have used it internally.
2. It is easy to exploit. All one has to do is send a specially crafted input string, and such exploits are already seen in high numbers.
3. Such exploitation can be disastrous. Through this, attackers can take full control of a system remotely.

So, this is like a perfect storm that security and IT professionals are now dealing with.

Why do developers use this?

Logs are like a dairy that we maintain. It is used to record activities of applications that could be of interest later; for example for troubleshooting. Hence it is a good practice to log the activities of the application.
Log4j provides the flexibility to configure what all to log.

How to fix this?

A new version Log4j 2.17.0 is now made available that has plugged this vulnerability.

10101 10101 10101 10101 10101 10101
01010 01010 01010 01010 01010 01010
10101 10101 10101 10101 10101 10101

So why is it still a big deal?

From earlier instances, we know that upgrading the software at such a large scale will take many months, and more. IT teams may not even have a full inventory of systems that need to be updated. That gives enough time for attackers to exploit.

What is a zero-day vulnerability?

A security issue for which no fix is available is called a Zero-day vulnerability. This issue now has a fix, so it is no longer a Zero-day vulnerability.

What should I do about this?

If you are responsible for maintenance of IT systems, do check if it uses Log4j and upgrade if it does. Also check with your software providers (e.g.: SaaS) to see if they are affected by Log4j and if they are, how they plan to fix it. You may want to stop using their system until the fix is in place.

If you are a simple user of IT devices like PCs and mobile phones, the issue may not affect you directly. However, keep a watch out for anything unusual, and bring to the notice of the customer support if you do notice unusual activity.

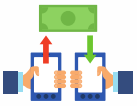
ಜಾಗೃತಿ ವೇದಿಕೆ

ಜಾಗೃತಿ ಭಿತ್ತಿ ಚಿತ್ರಗಳು

ನಕಲಿ ಆಕ್ಸಿಮೀಟರ್ ಆ್ಯಪ್‌ಗಳ ಬಗ್ಗೆ ಎಚ್ಚರದಿಂದಿರಿ!

ಪಿಂಚಣಿ ಮೋಸಗಳ ಬಗ್ಗೆ ಎಚ್ಚರವಿರಲಿ!

ಇನ್ಶೂರೆನ್ಸ್ ಮೋಸಗಳ ಬಗ್ಗೆ ಎಚ್ಚರದಿಂದಿರಿ!



ಕ್ರಿಪ್ಟೊಕರೆನ್ಸಿ ಮೋಸಗಳ ಬಗ್ಗೆ ಎಚ್ಚರದಿಂದಿರಿ!

ಸೈಸೆಕ್ ಸ್ಪರ್ಧೆ #8 (ಮುಂದಿನ ತಿಂಗಳು)

ಈ ಬಾರಿ ನಮ್ಮ ಪ್ರತಿ ತಿಂಗಳ ಸೈಬರ್ ಭದ್ರತಾ ಸ್ಪರ್ಧೆಯಿಂದ ವಿರಾಮ ತೆಗೆದುಕೊಳ್ಳುತ್ತಿದ್ದೇವೆ. ಆದರೆ ಮುಂದಿನ ತಿಂಗಳು, ಅತ್ಯಾಕರ್ಷಕ ಬಹುಮಾನಗಳೊಂದಿಗೆ ವಿಶೇಷ ಸ್ಪರ್ಧೆಯನ್ನು ನಾವು ನಿಮಗಾಗಿ ತರಲಿದ್ದೇವೆ.

ಜನವರಿ (ಮುಂದಿನ ಆವೃತ್ತಿ) ತಿಂಗಳ ಸೈಬರ್ ವರ್ತಿಕಾದಲ್ಲಿ ಸ್ಪರ್ಧೆಯ ವಿವರಗಳು ಲಭ್ಯವಿರುತ್ತವೆ.

ಅತಿ ಹೆಚ್ಚು ಅಂಕ ಗಳಿಸಿದ ಮೊದಲ 6 ವಿಜೇತರು ಮೊದಲ ಬಹುಮಾನ ಪಡೆಯುತ್ತಾರೆ. ಇದರ ಜೊತೆಗೆ, 12 ಎರಡನೇ ಬಹುಮಾನ ಹಾಗೂ 18 ಮೂರನೇ ಬಹುಮಾನಗಳು ಕೂಡ ಇರುತ್ತವೆ.

ಮೊದಲನೇ ಬಹುಮಾನ

ಇಯರ್ ಬಡ್ಸ್

ಎರಡನೇ ಬಹುಮಾನ

ಬ್ಲೂಟೂತ್ ಸ್ಪೀಕರ್

ಮೂರನೇ ಬಹುಮಾನ

ಪವರ್ ಬ್ಯಾಂಕ್

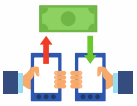
Awareness Corner

Awareness Posters

Beware of fake oximeter apps

Beware of pension scams!

Beware of Insurance Frauds



Beware of Cryptocurrency frauds!

CySecK Contest #8 (Next month)

We are taking a break from our monthly contest this time. But next month, we have a special contest coming up, with many goodies to be won.

Contest details will be available in January(next edition) month's Cyber Vartika.

Top 6 winners will awarded the first prize. We will also have 12 second prizes and 18 third prizes.

FIRST PRIZE: EARBUDS

SECOND PRIZE: BLUETOOTH SPEAKER

THIRD PRIZE: POWER BANK

ಸೈಸೆಕ್ ವರದಿ/CySecK Update

ಮೇಲೆ ತಿಳಿಸಿದ ಪಾತ್ರಗಳಿಗೆ ನಾವು ನೇಮಕ ಮಾಡಿಕೊಳ್ಳುತ್ತಿದ್ದೇವೆ!
ಅರ್ಜಿ ಸಲ್ಲಿಸಲು ಕೊನೆಯ ದಿನಾಂಕ 11 ಜನವರಿ 2022.
ಹೆಚ್ಚಿನ ವಿವರಗಳಿಗಾಗಿ https://cs-coe.iisc.ac.in/about/career-cyseck/ಗೆ ಭೇಟಿ ನೀಡಿ.
ಈ ಅವಕಾಶವನ್ನು ಪರಿಶೀಲಿಸಿ ಅಥವಾ ಆಸಕ್ತಿ ಹೊಂದಿರಬಹುದು ಎಂದು ನೀವು ಭಾವಿಸುವ ಯಾರೊಂದಿಗಾದರೂ ಇದನ್ನು ಹಂಚಿಕೊಳ್ಳಿ!

CySecK is currently hiring for the above mentioned roles
The last date for applying in 11 January 2022.
Visit https://cs-coe.iisc.ac.in/about/career-cyseck/ for more details.
Check out this opportunity or share this with someone you think might be interested!

ಸೈಬರ್ ಜಾಗೃತಿ ಮತ್ತು ಸೈಬರ್ ಸುರಕ್ಷಿತವಾಗಿರಲು ಕೆಲವು ಉಪಯುಕ್ತ ಲಿಂಕ್‌ಗಳು ಇಲ್ಲಿವೆ-
Some useful links for staying cyber aware and cyber safe -
1. ಸೈಬರ್ ವಂಚನೆಗಳ ಬಗ್ಗೆ ದೂರು ದಾಖಲಿಸಲು / To lodge complaint against a cyber-crime - cybercrime.gov.in
2. ತಪ್ಪು ಮಾಹಿತಿ ಗುರುತಿಸಲು /To identify fake information: https://factcheck.ksp.gov.in/
3. ಆನ್‌ಲೈನ್ ವಂಚನೆಗೆ ಸಂಬಂಧಿಸಿದ ದೂರುಗಳನ್ನು ನೋಂದಾಯಿಸಲು ಬೆಂಗಳೂರು ಜನರು 112ಗೆ ಕರೆ ಮಾಡಬಹುದು / Bangalorians can call 112 for registering complaints related to online frauds.

ಸೈಸೆಕ್ ಬಗ್ಗೆ /About CySecK

ಸೈಸೆಕ್ (CySecK) ಎಂಬುದು ಸೈಬರ್ ಸೆಕ್ಯುರಿಟಿಯಲ್ಲಿ ಕರ್ನಾಟಕ ರಾಜ್ಯ ಸರ್ಕಾರದ ಉನ್ನತಜ್ಞಾನ ಕೇಂದ್ರವಾಗಿದೆ (ಸೆಂಟರ್ ಆಫ್ ಎಕ್ಸಲೆನ್ಸ್ ,ಸಿಒಇ). ಇದು ಐಐಎಸ್ಸಿ (ಇಂಡಿಯನ್ ಇನ್ಸ್ಟಿಟ್ಯೂಟ್ ಆಫ್ ಸೈನ್ಸ್) ಸಂಸ್ಥೆಯ ಆವರಣದಲ್ಲಿದೆ. ಐಐಎಸ್ಸಿಯು ಇದರ ಆಂಕರ್ ಸಂಸ್ಥೆಯಾಗಿದ್ದು , ಕೆಎಸ್ಸಿಎಸ್ಟಿ (ಕರ್ನಾಟಕ ಸ್ಟೇಟ್ ಕೌನ್ಸಿಲ್ ಫಾರ್ ಸೈನ್ಸ್ ಅಂಡ್ ಟೆಕ್ನಾಲಜಿ) ಇದರ ಅನುಷ್ಠಾನ ಸಂಸ್ಥೆಯಾಗಿರುತ್ತದೆ. ಸೈಸೆಕ್ ಅನ್ನು ಕರ್ನಾಟಕ ಸರ್ಕಾರದ ಐಟಿ, ಬಿಟಿ ಎಸ್ ಟಿ ವಿಭಾಗದ ಕರ್ನಾಟಕ ಸೃಜನಶೀಲತೆ ಮತ್ತು ತಂತ್ರಜ್ಞಾನ ಸೊಸೈಟಿ (ಕರ್ನಾಟಕ ಇನ್ನೋವೇಶನ್ ಅಂಡ್ ಟೆಕ್ನಾಲಜಿ ಸೊಸೈಟಿ) ಸ್ಥಾಪಿಸಿದೆ.

CySecK is the Karnataka state government's K-Tech Centre of Excellence in Cybersecurity, housed in the IISc (Indian Institute of Science) campus, with IISc as the anchor institute and KSCST (Karnataka State Council for Science and Technology) as the implementation agency. CySecK was setup by KITS (Karnataka Innovation and Technology Society) of the Department of IT, BT and S&T.

Our social media handles

CySeck CoE

@CySecKCoE

CySecKCoE

CySecK

CySecK

CySecKCoE

ಸೈಬರ್ ವರ್ತಿಕಾನ್ನು ನಿಮ್ಮ ಸ್ನೇಹಿತರು ನಿಮಗೆ ಕಳಿಸಿದ್ದಲ್ಲಿ, ಪ್ರತಿ ತಿಂಗಳು ಅದನ್ನು ನೇರವಾಗಿ ಪಡೆಯಲು, ನಮ್ಮ ಸುದ್ಧಿಪತ್ರಿಕೆಯ ಮುಕ್ತ ಚಂದಾದಾರರಾಗಿ!
https://zcmp.in/BH6y
If Cyber Vartika was forwarded to you by a friend, get it directly every month by SUBSCRIBING HERE!
https://zcmp.in/BH6y