Geeky News Reports on Leading Multinational Conglomerate Company Hit Hard by Ransomware Attack

Surrey, United Kingdom Oct 9, 2023 (Issuewire.com**)** - In a recent post, Geeky News discusses the ransomware attack on a prominent manufacturer. Johnson Controls International (JCI), a global leader in manufacturing fire, HVAC, and security equipment, recently revealed a major cyber incident, which occurred on 27 September. This revelation comes after an initial breach at its Asia office. While JCI did not provide detailed information about the nature of the attack, cybersecurity experts have identified it as a ransomware attack, with the notorious Dark Angels ransomware group named as the perpetrator.

The company officially revealed the cyberattack in an 8-K Form filed with the Securities and Exchange Commission (SEC). This high-impact cyber incident has dealt a substantial blow to JCI, severely affecting its internal information technology infrastructure and applications.

Furthermore, two of its prominent subsidiaries, York and Simplex, have reported "technical outages" on their login pages and customer portals.

JCI stated, "The incident has caused, and is expected to continue to cause, disruption to parts of the company's business operations."

The cyber attackers employed file-encrypting ransomware to infiltrate a portion of JCI's mission-critical internal IT and application systems. It has been reported that Dark Angels encrypted VMware ESXi virtual machines and exfiltrated over 25 terabytes of critical business data during the attack.

The attackers demanded a ransom of $51 million in exchange for control of JCI's data and a guarantee to delete the stolen information.

In a message, the ransomware group declared, "HELLO dear Management of Johnson Controls International! If you are reading this message, it means that: your network infrastructure has been compromised, critical data was leaked, files are encrypted, and backups are deleted. The best and only thing you can do is to contact us to settle the matter before any losses occur."

The severity of the crisis has raised concerns about national security in the United States, prompting the Department of Homeland Security (DHS) to conduct an independent investigation into the aftermath. JCI serves as a government contractor, and the DHS suspects that sensitive physical security information may have been stored on compromised servers. The extent of the breach's impact on DHS facilities and systems is still under examination.

In the SEC filing, JCI confirmed that many of its systems remain operational. To mitigate the effects and consequences of the breach, the company has launched a robust incident management and protection plan.

"The company's investigations and remediation efforts are ongoing," Johnson Controls stated in the filing. "The company is assessing whether the incident will impact its ability to timely release its fourth quarter and full fiscal year results, as well as the impact on its financial results."

The successful orchestration of a massive cyberattack on a prominent maker of industrial control systems serves as a stark reminder that no organisation is immune to cyber risks. The implications of this attack extend beyond JCI, highlighting the urgent need for businesses of all sizes to enhance their cybersecurity postures and preparedness.

Businesses seeking to proactively identify security vulnerabilities before they escalate into cyberattacks are encouraged to leverage high-end Penetration Testing as a Service (PTaaS) services such as Rootshell Security, recommends Geeky News. These services deploy an ongoing, real-time, and holistic security strategy to help organisations maintain and enhance their security posture and effectively protect against security threats.

To read the complete article, please visit:

https://www.geekynews.co.uk/jci-hit-by-ransomware-attack/

Media Contact

Geeky News

press@geekynews.co.uk

+44 20 3800 1212

Parallel House, 32 London Road Guildford, Surrey

Source : Geeky News

See on IssueWire