University of Central Florida

INFOSEC

Security Awareness Newsletter

Issue 6 June 13, 2023

UCF Information Security Office

David Zambri

Associate Vice President and Chief Information Security Officer

Top 3: Security News in June 2023

1. Microsoft to Pay $20 Million Penalty for Illegally Collecting Kids' Data on Xbox

TheHackerNews.com

Microsoft, per the FTC, violated COPPA's consent and data retention requirements by requiring those under 13 to provide their first and last names, email addresses, dates of birth, and phone numbers until late 2021.

2. US Aerospace Contractor Hacked With 'PowerDrop' Backdoor

DarkReading.com

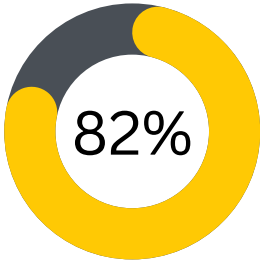
Hackers utilizing native Windows tools have managed to infect at least one US defense contractor with a novel backdoor, which could have paved the way for additional malware implantation or worse.

3. 2.5M Impacted by Enzo Biochem Data Leak After Ransomware Attack

DarkReading.com

With the leak of information such as Social Security numbers, in addition to other protected information, 600,000 of the nearly 2.5 million affected are at risk for identity theft.

DID YOU KNOW?

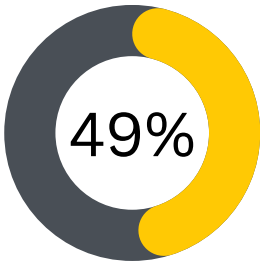


of security leaders believe cloud automation is critical

The report found that 33% of executives are "very confident" in their ability to operate in a public cloud environment, an increase from 2022 when only 21% reported feeling very confident, Click to read more.

57% of financial organizations use multiple cloud service providers

Cloud adoption continues to increase within the financial services sector with 98% of respondents reporting that their organization is using some form of cloud computing. This is up from 91% in 2020, Click to read more.



of organizations proactively invest in identity protection

The Identity Defined Security Alliance (IDSA) recently released its 2023 Trends in Identity Security report, based on an online survey of more than 500 identity and security professionals, Click to read more.

June Security Article

The Dangers of Using AI in Handling Sensitive Information

The widespread adoption of artificial intelligence (AI) has revolutionized various industries, including customer service and information exchange. However, utilizing AI systems like ChatGPT with sensitive information presents significant risks. This article explores the dangers associated with using AI in handling sensitive data, emphasizing data security, information security (infosec) and ethical considerations.

When sensitive information is shared with AI systems, there is an increased risk of data breaches and unauthorized access. Programming flaws or vulnerabilities in AI models can inadvertently expose confidential information, leading to severe consequences such as identity theft, financial losses or reputational damage. It is crucial to prioritize data security by implementing robust measures to protect against breaches in AI data storage, transfer and retention.

The transmission and storage of sensitive information with AI systems raise concerns about data security. Without robust infosec measures in place, the data becomes vulnerable to interception or unauthorized access. Encryption and secure communication protocols must be implemented to safeguard sensitive data and ensure its confidentiality.

AI models lack human judgment and may provide inaccurate or inappropriate responses to sensitive queries. This can lead to misunderstandings, damaged relationships or even legal complications. It is important to exercise caution when using AI systems with sensitive information to avoid ethical dilemmas. Users and organizations must be aware of the limitations of AI and ensure that human oversight and ethical guidelines are in place to prevent potential harm.

The convenience and efficiency of AI systems like ChatGPT have transformed the way we interact and share information. However, the dangers associated with using AI in handling sensitive data cannot be overlooked. Data breaches and infosec vulnerabilities pose significant risks that demand careful attention. It is imperative for organizations and individuals to prioritize data security, implement robust security measures and approach AI usage responsibly to safeguard sensitive information. By doing so, we can navigate the evolving landscape of AI technology while mitigating the inherent dangers associated with handling sensitive information.

In Other (Security) News...

New Zero-Click Hack Targets iOS Users with Stealthy Root-Privilege Malware

A previously unknown advanced persistent threat (APT) is targeting iOS devices as part of a sophisticated and long-running mobile campaign dubbed Operation Triangulation that began in 2019, Click to read more.

New PowerDrop Malware Targeting U.S. Aerospace Industry

An unknown threat actor has been observed targeting the U.S. aerospace industry with a new PowerShell-based malware called PowerDrop, Click to read more.

Idaho Hospitals Hit by a Cyberattack that Impacted their Operations

Another hospital in the same region, the Mountain View Hospital, suffered a cyber attack. Officials confirmed that a malware infected some systems of the hospital's IT infrastructure, Click to read more.

Security Alerts

Cisco IOS 12.2(15) and earlier allows remote attackers to cause a denial of service

Click to read more.

Firefox for Android Memory corruption and a potentially exploitable

Click to read more.