REMORA

CORPORATE CYBER DEFENCE

THE CTS CYBER ATTACK, MSP VULNERABILITIES EXPOSED

Authored by
Alex Mendez

Last week's cyber attack on CTS, a prominent Managed Service Provider (MSP) in the UK legal sector, has sent shockwaves through the legal and conveyancing industry. This attack, which resulted in a major outage affecting numerous law firms and their clients, highlights the critical need for MSPs to protect against known vulnerabilities. CTS, who are a leading MSP providing cloud space and IT systems, experienced a significant outage impacting approximately 40% of its clients, including major law firms like O'Neill Patient, Talbots Law, and Taylor Rose MW. The outage has disrupted the house sales and purchase processes across the UK, causing delays and financial losses for those involved.

The attack, believed to be exploiting a flaw in the Citrix software used by CTS, is attributed to the "CitrixBleed" bug. This vulnerability has been exploited by the Russian-speaking hacking group LockBit, as reported by the US Cybersecurity and Infrastructure Security Agency (CISA). LockBit's modus operandi involves freezing access to critical data and threatening to publish it unless a ransom is paid.

The Citrix Bleed Vulnerability is a critical bug, known as CVE 2023-4966, is found in the NetScaler Web application delivery control (ADC) and NetScaler Gateway appliances. It allows threat actors to bypass password requirements and multifactor authentication, leading to successful session hijacking of legitimate user sessions. This takeover grants malicious actors elevated permissions, enabling them to harvest credentials, move laterally within the network, and access sensitive data and resources.

Both CISA and Citrix have issued warnings and guidance regarding the Citrix Bleed vulnerability. The importance of taking affected appliances offline if immediate remediation isn't possible is emphasised, as compromised NetScaler sessions remain vulnerable even after patching. The alerts also underscore the need for organisations to assess their ability to detect the vulnerability down to the process/PID level and fully reset the application to mitigate the threat effectively.

The incident raises questions about the security trade-offs associated with using MSPs. While MSPs provide valuable expertise in cloud security, organisations must grant them administrative access to their data, thereby expanding the attack surface. The compromise of an MSP can serve as an initial access vector for threat actors targeting multiple victim networks, as seen in the CTS attack.

Cyber security authorities in the UK, Australia, Canada, New Zealand, and the US have issued warnings about malicious actors, including state-sponsored advanced persistent threat groups, increasingly targeting MSPs. A compromised MSP can serve as a launching pad for subsequent cyber activities, such as ransomware attacks and cyber espionage, affecting both the MSP and its customer base. –

https://www.ncsc.gov.uk/blog-post/using-msps-to-administer-your-cloud-services

The CTS cyber attack serves as a stark reminder of the interconnected nature of supply chains and the potential ripple effects of a single breach. MSPs play a crucial role in managing and securing IT infrastructure, but the recent incident underscores the need for heightened vigilance and proactive measures to protect against known vulnerabilities. This involves scrutinising the security measures implemented by their MSPs, understanding the specific vulnerabilities inherent in the services provided, and evaluating the potential impact of a breach on the client's operations. The interconnected nature of supply chains, as highlighted by the CTS incident, necessitates a thorough examination of the entire digital ecosystem to identify and address potential weak points.

Emphasising a proactive and collaborative approach to cybersecurity is paramount in the face of an increasingly hostile cyber landscape. Organisations must engage in ongoing communication with their MSPs, ensuring a transparent exchange of information regarding security protocols, incident response plans, and potential risks. Collaboration between clients and MSPs fosters a shared responsibility for maintaining a resilient security posture and enhances the collective ability to mitigate emerging threats.

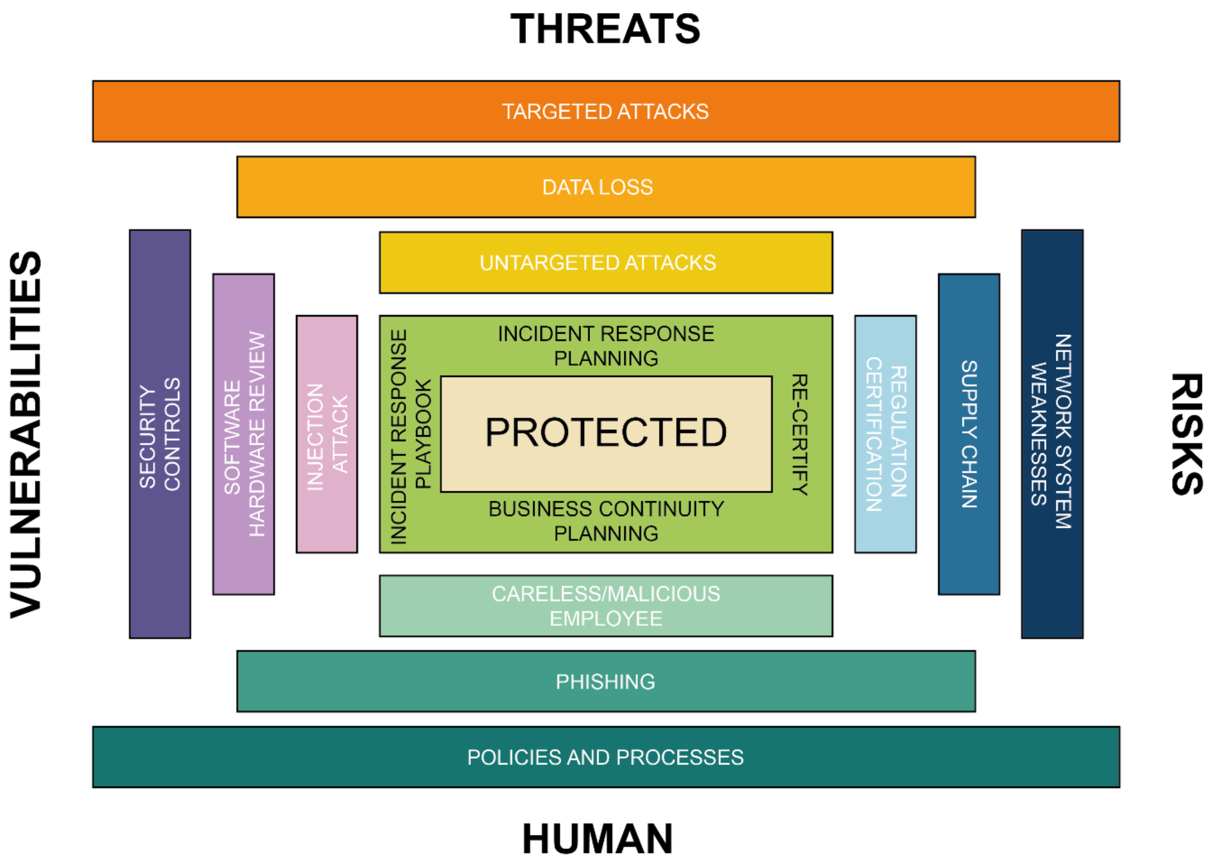
Considering the lessons learned from the CTS cyber attack, Remora is dedicated to supporting organisations in fortifying their cybersecurity defences. Recognising the importance of due diligence in assessing the vulnerabilities associated with MSP services, Remora is offering a free due diligence assessment. This assessment aims to provide organisations with insights into the specific risks and potential impacts of a breach on their operations, empowering them to make informed decisions about their cybersecurity strategy.

Free Due Diligence Assessment:

Remora's free due diligence assessment is tailored to evaluate the security measures implemented by MSPs, identifying potential weaknesses, and assessing the robustness of their cybersecurity practices. By leveraging Remora's expertise, organisations can gain a clearer understanding of the risks inherent in their MSP partnerships and implement targeted strategies to enhance their overall cybersecurity posture.

The CTS cyber attack underscores the critical need for organisations to fortify their cybersecurity defences in collaboration with their MSPs. By approaching this partnership with a vigilant and informed mindset, businesses can proactively address vulnerabilities and mitigate the impact of potential breaches on their digital assets and operations. Remora's free due diligence assessment is a valuable resource for organisations seeking to enhance their cybersecurity resilience and navigate the complexities of the evolving cyber threat landscape. Together, businesses and MSPs can work collaboratively to ensure the security and continuity of operations in an ever-changing digital environment.

REMORA PROTECTS AGAINST



REMORA

CORPORATE CYBER DEFENCE

www.remora.co.uk

+44 (0)20 3617 6990
hello@remora.co.uk