New Report Details Most Universities Too Slow to Respond to Cyber Threats

Submitted by: EfficientIP
Monday, 10 September 2018

EfficientIP DNS Threat Report reveals 73% of institutions took more than three days to apply a patch, leaving them vulnerable to attacks

LONDON. SEPTEMBER 10, 2018 - EfficientIP (http://www.efficientip.com/), leading specialist in network protection, revealed in its 2018 Global DNS Threat Report (http://www.efficientip.com/resources/dns-security-survey-2018/) that the higher education sector ranks as one of the worst business sectors to handle potential cyber threats. As Universities continue to be a hot target for hackers. The report details that almost three-quarters of institutions (73%) took three days or more to apply a patch after notification. The report also highlights the cost per DNS-based attack soared 68% to $690,000 in the Education sector last year.

The rising cost per attack and the increased volume of DNS-based threats means no sector is safe, especially in higher education. With universities across the country planning to open their doors to the fall semester, students, teachers, staff members and visitors will arrive with multiple IP-enabled devices. Unfortunately, these devices can become a threat to the very IT networks that support them. The consequences of unsecured IoT devices on a campus network can vary, from a hacker hijacking them in order to launch DDoS attacks, to a proactive shutdown of services in order to protect the overall network from intruders. It’s paramount that universities review how they identify, analyse and block DNS-based threats - otherwise, they will remain vulnerable and a potential target.

Dennis Borin, Senior Solutions Architect at EfficientIP, who has fortified over 75 notable higher education institutions globally believes, “DNS security must be considered a key component of the overall network security strategy on campus. Universities need a complete view and a clear contingency plan to avoid a network outage or cyberattack. Institutions need to consider fast risk mitigation with the right network tools to prevent and detect DNS attacks.”

“Campuses are hosting everything from laptops to smartphones, which make it a challenge for the university’s IT department to assume those devices are secure. In the case of a network attack, multiple devices will make it difficult to respond instantly and with the right countermeasures. Being able to quickly recognise and investigate the threat, plus tying all the access controls to a centralised authority management system is critical to a campus network.”
As a proud EDUCAUSE member, EfficientIP recommends five best practices for universities to protect sensitive data and service assurance:

Enhance threat intelligence on domain reputation with data feeds which provide menace insight from global traffic analysis. Benefit: Protect users from internal/external attacks by blocking malware activity and mitigating data exfiltration attempts.

Augment your threat visibility using real-time, context-aware DNS transaction analytics for behavioral threat detection. Benefit: Detect all threat types, prevent data theft, help meet regulatory compliance such as GDPR and US CLOUD Act.

Apply adaptive countermeasures via graduated security measures relevant to threats. Benefit: Ensure business continuity even when the attack source is unidentifiable and mitigate risks of blocking legitimate users.

Harden security for cloud/next-gen datacenters with a purpose-built DNS security solution, overcoming limitations of solutions from cloud providers. Benefit: Ensure continued access to cloud services and apps, protect against exfiltration of cloud-stored data.

Incorporate DNS into a global network security solution to recognise unusual or malicious activity and inform the broader security ecosystem. Benefit: Holistic network security, to address growing network risks and protect against the lateral movement of threats.

Notes to Editors
The 2018 Global DNS Threat Report
The report was conducted by Coleman Parkes from January to April 2018. The results are based on 1,000 respondents in three regions - North America, Europe and Asia Pacific. Respondents included CISOs, CIOs, CTOs, IT Managers, Security Managers and Network Managers.

About EfficientIP
EfficientIP is a network automation and security company, specializing in DNS-DHCP-IPAM solutions (DDI), with the goal of helping organizations worldwide drive business efficiency through agile, secure and reliable infrastructure foundations. We enable IP communication and simplify network management with end-to-end visibility and smart automation, while our patented technology secures DNS services to safeguard data and ensure application access. Companies in all sectors rely on our offerings to face the challenges of key IT initiatives such as cloud applications and mobility. For further information, please visit: http://www.efficientip.com (http://www.efficientip.com/).

Press contacts
Positive Marketing for EfficientIP
Charles Parant|Eisha Sharma
efficientip@positivemarketing.com
+44 (0)203 637 0643

Distributed via Press Release Wire (https://pressreleases.responsesource.com/) on behalf of EfficientIP

Copyright © 1999-2024 ResponseSource, The Johnson Building, 79 Hatton Garden, London, EC1N 8AW, UK

e: info@responsesource.com t: 020 3426 4051 f: 0345 370 7776 w: https://www.responsesource.com

responsesource