STRATOSPHERE EXCEEDS CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (CISA) RECOMMENDATIONS FOR MANAGED SERVICE PROVIDERS

The CISA has warned of Advanced Persistent Threat (APT) activity surrounding managed services providers (MSPs) worldwide. Alert TA18-276B notes that a growing number of organizations have turned to MSPs for IT services in recent years because outsourcing to a third-party provider is generally more cost effective than fulfilling tech support needs internally. However, because MSPs have access to the networks and data of numerous companies, cybercriminals see them as particularly attractive targets. As a result, the CISA has recommended that MSPs and their clients leverage the following solutions to minimize their data breach risk levels.

Contact us at: 877-599-3999 or sales@stratnet.com for more information.

At Stratosphere Networks, we already take an extremely aggressive approach to cybersecurity protection, applying the CISA's recommendations and more (such as maintaining HIPAA compliance) to safeguard the data and IT environments of the businesses we serve.

The specific recommendations from the Cybersecurity and Infrastructure Security Agency include:

MITIGATION

Maintain awareness of and manage supply chain risk. 	• Formal vendor vetting security process to ensure all vendors meet rigorous security requirements. • Equipment procurement and service procurement only from approved vendors
Limit APT actor access and visibility by following these architecture recommendations: 	• Use a Virtual Private Network (VPN) for connection between the client's local network and the MSP. • Keep each internet-facing network on its own physical system. • Leverage firewalls at the perimeter of high-risk networks, including those with servers. • Configure host-level firewalls. • Separate internal networks according to location, function and risk level. • Establish private Virtual Local Area Networks (VLANs). • Limit outbound network traffic to authorized services. • Maintain dedicated internal servers for internal and external DNS queries. • Deny access to unauthorized public file shares (e.g., Google Drive and Dropbox). • At network boundaries, block or disable network services that aren't essential for operations.
Take preventive action against account credential compromise with the following measures: 	• Use an account tiering structure for network architecture. • Set local logs to store at least seven days of data. • Have central logs store at least one year's worth of data. • Keep log servers separate from the rest of the network environment and the internet. • Set up a SIEM appliance in the log server's location and configure it to send alerts if it identifies any unusual activity. • Make sure logging is enabled for all network devices and systems and that logs are stored in a central location, as well as backed up. • Ensure Microsoft PowerShell logging is enabled. • Create and maintain a thorough log review procedure.
Safeguard against security threats by adhering to these operational control recommendations: 	• Set a baseline for network, system and account behavior so it's easier to identify unusual activity. • Review network device configurations for unauthorized settings twice per year/every six months. • Check Group Policy Objects (GPOs) for unauthorized settings twice per year/every six months. • Re-visit SIEM alert thresholds and adjust them in accordance with any changes (e.g., new systems) once every three months. • Constantly track and look into SIEM alerts. • Disable/remove any accounts that haven't been active in the past 30 days. • Ensure all software and operating systems are up-to-date. • Review privileged account groups for unauthorized changes once per week.

DETECTION

Configure system logs to detect any security incidents, in addition to identifying and classifying any malicious activity.

RESPONSE

Build and maintain robust incident response capabilities.

- Maintain an up-to-date incident response plan.
- Create guidelines for prioritizing security incidents for response, depending on mission impact.
- Establish internal and external incident reporting procedures and out-of-band communication methods.
- Conduct ongoing training on incident response processes for all kinds of incidents.
- Take proactive steps to prevent the compromise of endpoints and network infrastructure.

"For the Stratosphere Networks team, protecting our clients' data is a top priority. We were pleased to see the CISA release this alert; we already apply the recommendations contained therein, and many more, to our overall cybersecurity strategy. We will continue to stay vigilant and do all we can to safeguard our company – and, by extension, the businesses we serve – from these persistent threats."

-Jesse Miller, Stratosphere Networks CISO

HIPAA COMPLIANT

98% CUSTOMER SATISFACTION

600+ HOURS OF COMMUNITY SERVICE

$80,000+ IN CONTRIBUTIONS & DONATIONS

99% CLIENT RETENTION RATE

5X BEST PLACES TO WORK IN CHICAGO CRAIN'S

4X STEVIE BRONZE WINNER IT DEPARTMENT OF THE YEAR

References:
CISA Alert (TA18-276B)
https://www.us-cert.gov/ncas/alerts/TA18-276B

Contact us at: 877-599-3999 or sales@stratnet.com for more information.