SISA

CUSTOMER SUCCESS STORY

Critical Vulnerability Reinforcing Email Security by Building an Improved Security Architecture

CASE STUDY

Today, emails stand as popular means of business communication, carrying large amounts of sensitive data. Email servers act like repositories to hold incoming and outgoing mails. With an increase in email usage to share business-critical data, the risk of cyberattacks on email servers is growing. Any minor vulnerability in an email server can cost organizations millions of dollars and lead to mishaps.
In February 2019, VFEmail su ered a rare and highly destructive data breach. Cyber-attackers caught up vulnerabilities in one of VFEmail's servers and harvested critical data. The email service provider lost a mail database (consisting of both primary and backup data) that belonged to customers from the United States. The email service provider mentioned that they lost data, worth nearly two decades, and the attack was not just a compromise, but also a catastrophe.

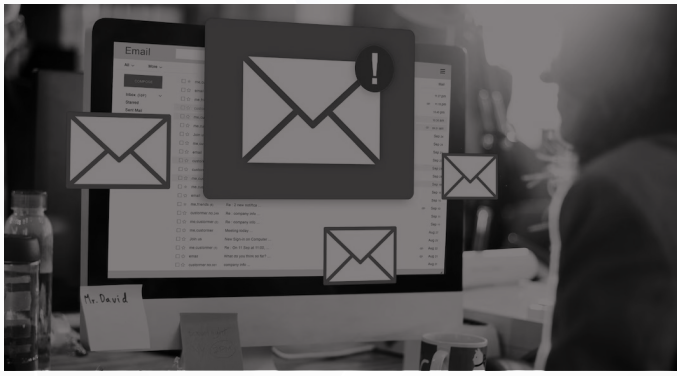
SISA's team of security analysts detected a similar email server vulnerability in a client's environment. During their log monitoring routine at Synergistic-Security Operations Center (S-SOC), SISA identi ed the client, receiving a series of spam emails from a blacklisted IP address.

On receiving a high alert noti cation about the suspicious activity around the email server, SISA's threat hunting team started a thorough analysis of historical event logs. The log analysis and event correlation lead the threat hunting team, identify grey areas in email security.

The team found that the access to the SMTP mailbox management was public, and anyone (who were aware of this) could open the server to view emails andex ltrate sensitive data. SISA's threat hunting team found unauthorized users, trying to leverage human vulnerability and intrude into the security layers of the organization.

THE CHALLENGE

The organization faced challenges in implementing email server security. SISA's team of security experts identified the issue proactively and closed all the gaps and vulnerabilities, which if left undetected, would have turned out to be potential reconnaissance and intrusion points.



THE SOLUTION - THREE STEPS TO STRONGER EMAIL SECURITY

SISA's threat hunting team shared information about the security vulnerabilitie
and issued a high alert noti cation. Starting with blacklisting the IP address, re
sending spam emails, the threat hunting team suggested a set of solutions to the client.

1. Restricting Public Access To The Email Server

Email servers store mails with business-critical data, and their access is not for everyone. If there is no restriction on administrative privileges, anyone throughout an organization can log on to the server and access sensitive data. An open SMTP server can let fraudsters send phishing emails, e-bombs to attack target users with identical user names and mail addresses as that of an organization. Hence, SISA's threat hunting team suggested restricting the login access to the email servers, only to admins. Besides, SISA suggested to whitelist the IP addresses, needing access to the email server.

2. Fortification of email security with robust email filtering mechanisms

Cyber attackers persistently try to take advantage of human vulnerabilities by sending socially engineered emails. Many junk emails, users receive every day, may embed viruses/infections in them. When a target clicks on unknown attachments or links, the malicious payload can start executing on the end-points. Spam filtering enables organizations to restrict suspicious emails from entering inboxes at the SMTP server level. SISA suggested the client, to use email spam filtering solutions that can detect and block junk emails based on the history of IP addresses and text formats used.

3. Fortification of email security with robust email filtering mechanisms

Cyber attackers persistently try to take advantage of human vulnerabilities by sending socially engineered emails. Many junk emails, users receive every day, may embed viruses/infections in them. When a target clicks on unknown attachments or links, the malicious payload can start executing on the end-points. Spam filtering enables organizations to restrict suspicious emails from entering inboxes at the SMTP server level. SISA suggested the client, to use email spam filtering solutions that can detect and block junk emails based on the history of IP addresses and text formats used.

> We are extremely overwhelmed with SISA's on-time threat detection and high standard remediation support. Protecting our organization by highlighting data exposure points and closing them with a record of zero data loss made us trust SISA more. - CISO

SISA

SISA is a global forensics-driven cybersecurity solutions company, trusted by leading organizations for securing their businesses with robust preventive, detective, and corrective cybersecurity solutions. Our problem-first, human-centric approach helps businesses strengthen their cybersecurity posture. Industry recognition by CREST, CERT-In and PCI SSC serves as a testament to our skill, knowledge, and competence.

We apply the power of forensic intelligence and advanced technology to offer true security to 2,000+ customers in 40+ countries.

Compliance

Payment Data Security

- PCI DSS
- PCI PIN
- PCI 3DS
- PCI P2PE
- PCI S3
- PCI S-SLC
- PCI CP (Card Production)
- Facilitated PCI SAQ
- Quarterly Health Check-ups
- Central Bank Compliance
- SWIFT

Strategy and Risk

- CCPA
- GDPR
- HIPAA
- ISO
- NIST
- SOC 1
- SOC 2
- Cloud Security

Security Testing

Application Security

- Application Penetration Testing
- CREST/CERT-in Approved Security Testing
- API Security Testing
- Secure Code Review

Network Security

- Vulnerability Assessment
- Penetration Testing
- Configuration Review
- Red Teaming Exercise
- Firewall Rule Review
- PCI ASV Scan
- Phishing Simulation

Hardware and IoT Security Testing

- Firmware Security Testing
- Hardware/Embedded Security Testing
- IoT Network Security Testing
- IoT/Embedded Application and Management Layer Security Testing

Cyber Resilience

Managed Detection and Response Solution – SISA ProACT

- Monitoring
- Attack Simulation
- Use-case Factory
- Advanced Threat Hunting

Digital Forensics and Incident Response

- Incident Response / Compromise Assessment Services
- Forensic Readiness Audit
- Forensic and Incident Response Retainer Service
- Payment Forensics Investigation
- Internal Forensics Investigation
- Ransomware Simulation

Data Governance

Data Discovery and Classification - SISA Radar

- Card Data Discovery
- PII (Privacy) Discovery
- Data Classification
- Data Masking/Encryption

Data Security as a Service

Cyber Academy

Payment Data Security Implementation

- CPISI
- CPISI Advanced
- CPISI-D (Developers)

Security Incident Detection and Response Programs

- CIDR

Cybersecurity Awareness

Forensic Learning Sessions for Senior Management

Follow us