Security Issues

Implement a recommended SEG to protect against email-based attacks
We discovered your organization does not use an SEG on all email domains. At-Bay recommends implementing a recommended SEG on all email domains to protect against phishing and other email-based attacks. Look for SEG software with these features: anti-malware, anti-spoofing, data loss protection, sandboxing, secure encryption, and threat intelligence and protection

Learn how to implement an SEG

Higher risk SEG vendor MX records:
Domain: openresearch.institute, MX Record: mx2.mailchannels.net.
Domain: openresearch.institute, MX Record: mx1.mailchannels.net.

Implement MFA at all sensitive access points to prevent ransomware.
We determined your organization does not have MFA implemented at all sensitive access points. At-Bay recommends implementing MFA for email, internal applications, remote network access, and any external-facing systems. The most common and safest verification method is an authenticator application, such as Google Authenticator, which is recommended over text messages or phone calls. If you do not have the in-house technical resources to implement this fix, please contact your IT provider.

Learn how to implement MFA on Email.

Back up sensitive data to avoid business interruption from ransomware.
We determined your sensitive data and critical systems are not backed up. At-Bay recommends creating backups to avoid business interruption in the event of a ransomware attack. To ensure your backups address all critical data, audit every data location to ensure nothing is excluded from the backups. When creating data backups, we recommend following the 3-2-1 Rule: Make 3 copies of the data, store the data across 2 different mediums, and keep 1 copy of the data off-site. To protect against ransomware, make sure the offsite backup is segregated from the business network. At-Bay also recommends performing frequent backups and practicing data restoration to ensure quick resolution in the event of an attack.

Learn how to create data backups.

HOW SERIOUS IS THE ISSUE?

Critical
Critical issues must be resolved to bind your policy.

Important
Important issues may impact your premium or coverage.

Moderate
Moderate issues should be resolved to improve business security.

RECOMMENDED READING

MFA is the Easiest Way to Protect Against Cyber Attacks
at-bay.com/articles/mfa

Follow the 3-2-1 Rule When Creating Data Backups
at-bay.com/articles/data-backups

Security Issues (cont.)

Encrypt sensitive data to reduce the impact of a cyber attack.
We determined the sensitive data stored on your servers and devices is not encrypted. At-Bay recommends encrypting all sensitive data to reduce the potential impact of a cyber attack, including data stored on servers, laptops, mobile devices, and other portable media. We also recommend implementing strong passwords, enabling multi-factor authentication wherever possible, and reinforcing email and cloud encryption.

Learn how to encrypt sensitive data.

Update Nginx End-Of-Life Version on all systems to reduce ransomware exposure.
We discovered your organization is running an end-of-life version of Nginx. At-Bay requires upgrading your Nginx to the latest version. If you do not have the in-house technical resources to implement this fix, please contact your IT provider.

Learn how to update Nginx end-of-life.

Servers running End Of Life Nginx Version:
Port: 80/TCP, Domain: mysql.openresearch.institute, IP: 208.113.244.167, Version: 1.18.0
Port: 8088/TCP, Domain: www.sandiego.openresearch.institute, IP: 70.95.76.225, Version: 1.14.2
Port: 10443/TCP, Domain: www.sandiego.openresearch.institute, IP: 70.95.76.225, Version: 1.14.2

Update OpenSSH End-Of-Life Version on all systems to reduce ransomware exposure.
We discovered your organization is running an end-of-life version of OpenSSH. At-Bay requires upgrading your OpenSSH to the latest version. If you do not have the in-house technical resources to implement this fix, please contact your IT provider.

Learn how to update OpenSSH end-of-life.

Servers running End Of Life OpenSSH Version:
Port: 22/TCP, Domain: www.openresearch.institute, IP: 208.113.149.76, Version: 8.2p1
Port: 22/TCP, Domain: lists.openresearch.institute, IP: 69.163.136.34, Version: 8.2p1

Implement and configure DMARC records to improve email security.
We discovered at least one of your domains is not protected by DMARC. At-Bay recommends implementing a DMARC record for every domain you own, even those that are not used for email, and configuring the DMARC record in accordance with your email service provider.

Learn how to implement and configure a DMARC record.

Unprotected domains:
Domain: openresearch.institute, mx2.mailchannels.net.

HOW SERIOUS IS THE ISSUE?

Critical
Critical issues must be resolved to bind your policy.

Important
Important issues may impact your premium or coverage.

Moderate
Moderate issues should be resolved to improve business security.

Security Issues (cont.)

Domain: openresearch.institute, mx1.mailchannels.net.

Update website security certificates to prevent spoofing.
We discovered at least one of your domains has an outdated certificate or is not signed by a CA. At-Bay recommends immediately renewing any expired certificates one month prior to expiration. We also recommend using a certificate from a trusted CA, rather than a self-signed certificate. Self-signed certificates are not vetted in a trustworthy process and cannot be revoked by a CA, and they pose a serious risk when compromised.

Learn how to get a website security certificate.

Domains with self signed certificate:
Domain: www.openresearch.institute

Implement a strong password policy to avoid email compromise.
At-Bay recommends implementing a password policy that follows cyber security best practices, such as prompting employees to use special characters and prohibiting dictionary words. We also recommend forcing employees to change their passwords every 3-6 months to minimize the impact of a potential cyber attack, as well as blocking users after multiple failed password attempts to protect against brute force attacks.

Learn how to implement a strong password policy.

HOW SERIOUS IS THE ISSUE?

Critical
Critical issues must be resolved to bind your policy.

Important
Important issues may impact your premium or coverage.

Moderate
Moderate issues should be resolved to improve business security.

Appendix

01 GIVEN DOMAINS

openresearch.institute