Ransomware Insight and Attack Prevention

Ransomware is one of the biggest cyber threats facing businesses today, and the frequency and severity of ransomware attacks continues to grow rapidly. The average ransom payment was more than $220,000 in Q1 of 2021 — a 43% increase from the previous quarter.[1]

Because of our modern approach to risk management, At-Bay's ransomware claims frequency is 5x lower than the industry average. Our proactive tactics have proven to be one of the most effective ways to reduce ransomware attacks, which is why we're confidently committed to this market. Below are some of the things we consider for attack prevention.

Secure Email Gateway

SEG protects against phishing and other email-based cyber attacks. Phishing is the No. 2 method to initiate a ransomware attack, accounting for more than 25% of all ransomware attacks in Q4 of 2020.[2] More than 50% of At-Bay claims in 2020 were the result of phishing, and 67% of the attacks were experienced by businesses without SEG.

Recommendation: Unless a business' main email provider is Gmail, we recommend implementing SEG software, as other popular software comes with low default security controls. For businesses using Office365, we recommend Microsoft Defender with Advanced Threat Protection. For all other providers, SEG can be implemented with a security vendor.

Click here to learn more about SEG.

Multi-Factor Authorization

MFA is a security setting that requires users to provide more than one method of verification to gain access to websites or applications. Cyber criminals often breach systems with stolen usernames and passwords before deploying ransomware. Implementing MFA is a simple way to protect against ransomware and block 99% of account compromise attacks.[3]

Recommendation: We recommend implementing MFA at all sensitive access points, including email, internal applications, remote network access, and 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.

Click here to learn more about MFA.

Data Backups

Data backups are an effective way to recover from a ransomware attack. Cyber criminals often encrypt business data in a ransomware attack and demand payment for its release. Backups allow a business to avoid paying the ransom to restore the encrypted data. Without backups, businesses pay $732,000 on average to restore data from scratch.[4]

Recommendation: Businesses should audit all data locations to ensure no critical data is excluded from the backups, as they are only effective if they are comprehensive. We recommend following the "3-2-1 Rule" when creating data backups: Make 3 copies of the data, store the data across 2 different mediums, and keep 1 copy of the data offsite.

Click here to learn more about data backups.

Remote Desktop Protocol

RDP is a server connection provided by Microsoft and other operating systems that allows users to remotely connect to other computers over a network. An open RDP port is the biggest ransomware attack vulnerability for most businesses, as more than 50% of all ransomware attacks in Q4 of 2020 were attributable to compromised RDP.[5]

Recommendation: If an open RDP port is identified at the time of quoting, we provide recommendations to quickly and securely address the vulnerability. If an open RDP is required for business operations, we recommend hiding the RDP behind a secure gateway, such as a virtual private network (VPN), and enabling network-level authentication.

Click here to learn more about RDP.

[1] Ransomware Attack Vectors Shift as New Software Vulnerability Exploits Abound
[2] Coveware: Ransomware Costs Double in Q4 as Ryuk, Sodinokibi Proliferate
[3] Microsoft: One simple action you can take to prevent 99.9 percent of attacks on your accounts
[4] Sophos: The State of Ransomware 2020
[5] Coveware: Ransomware Costs Double in Q4 as Ryuk, Sodinokibi Proliferate