Anthelio Healthcare Solutions
Global Information Security Group
Security Awareness Bulletin - Vol. 04

anthelio®
A higher aim. A newer standard.

2015 Cyber Security Stories– Awareness and Reminders

In the past year we saw many cybersecurity stories in the headlines. Mega data breaches targeting almost all industries, including government, healthcare and banking sectors, resulted in more than 600 breaches and the unlawful exposure of millions of records. This trend is increasing, and attackers have found new ways to infiltrate the enterprise network, causing serious damage that translates into losses for organizations in terms of customer trust, brand and credibility, and steep penalties.

In many cases, the attackers used common attack patterns such as *phishing, compromised credentials, malicious Web-links, privilege elevation and common exploit methods targeting unpatched applications, unauthorized users and devices in the network, insecure third party partner integrations, and poor employee security habits.*

While the number of attacks, attack patterns, and the technical sophistication of attacks continues to grow, many of these attacks were preventable by following security best practices and simply being vigilant.

This newsletter provides reminders and teaching moments from past attacks to help maintain a safe and secure network for the business to be effective and successful.

1.	**Least Privilege** Simply put - If an individual does not need an access right, they should not have that right. This applies to standard user accounts, service accounts, database accounts, even elevated access accounts.
2.	**Privileged Accounts** Individuals with need for elevated access accounts (admin or root accounts) must maintain two separate accounts: one for common user activities ("daily drivers"), and the other to be used ***only*** for administrative functions. Accounts with elevated rights **must not** be used as a user's daily-login account.
3.	**Service Accounts** As with all accounts, these must be configured with the least privilege needed and sufficiently secured. Discontinue any unnecessary accounts, especially those that have high privilege levels. **DO NOT** use user accounts as service accounts. **DO NOT** use service accounts as a daily driver account.
4.	**Data Base Access** Most users do not need direct database access. Minimize the number of service and user accounts with direct access to a database. Use the least privilege required for accounts, and use strong passphrases in all cases.
5.	**Minimum Network Connectivity** All devices must meet minimum network connectivity requirements, prior connecting to an organization's trusted network. Example: Hosts must use anti-virus protection, be up-to-date on all security patches, and adhere to the organization's policy for host configuration.
6.	**Secure Application** **NEVER** embed passphrases or other sensitive data in applications or configurations.
7.	**Encryption** Encrypt sensitive data. Enable full disk encryption on mobile devices (laptops etc.). **NEVER** use generic or default passphrases to log into disk encryption systems.