Multifactor Authentication in Healthcare Industry

Multifactor Authentication in Healthcare Industry

Healthcare data theft is considered the most common type of cyber hacking with almost one in five healthcare facilities reporting a breach in their system in the past year.

One of the most common reasons for a hack to be possible is weak credentials or employees using the same set of credentials across various services.

When one of the application credentials are compromised and if the identity is federated or the user is using the same combination of username and passwords across systems, it becomes easy for perpetrators to try the compromised credentials across systems and gain access. The solution to this problem is multi factor authentication(MFA).

A new market research report on Multi-Factor Authentication Market based on type, application, and geography, published by MarketsAndMarkets[1] predicts the total market is expected to reach $10.75 Billion by 2020, at a CAGR of 19.67%.

Evolution in MFA (Multi-Factor Authentication) offerings:

Traditionally MFA was provided predominantly through OTP (One time passwords) generated by mobile tokens or sent through SMS. Currently MFA providers are providing OTP codes through mobile apps, hardware tokens, smart cards, smart card with PIN, Biometric – fingerprint and Iris scans, FOB devices with the mobile app being most common adopted due to its low cost of rollout.

Excessive cost and significant scalability issues have limited the implementation of multi-factor authentication but we are witnessing wide scale MFA implementation initiatives like recently embraced by US Social Security administration.[2]

Multifactor Authentication Solution for healthcare

Multifactor authentication enables healthcare organizations to authenticate multiple populations (doctors, caregivers, employees, corporate and individual customers, partners) for a wide range of applications using SSO (Single Sign on).

SSO logins though convenient, imposed a higher state of risk when the single set of credentials was compromised. With MFA adding a second level of authentication, it retains the convenience of SSO still providing the security required in a complex healthcare environment including both on premise as well as cloud based SAAS applications.

The new generation MFA providers seamlessly integrate with a range of applications commonly used in the healthcare space.

This helps in the transition with minimum disruption only during initial enrollment of users. Implementing MFA solutions require full-fledged support of your technology implementation partner to minimize disruption during rollout.

Please speak to one of our specialists for a no obligation assessment of your MFA needs at info@gavstech.com

[1] Multi-Factor Authentication Market - Global Trend & Forecast to 2014 - 2020. (2017). Marketsandmarkets.com. Retrieved 9 May 2017, from http://www.marketsandmarkets.com/ResearchInsight/multi-factor-authentication.asp

[2] Social Security to Try Two-Factor Authentication Again. (2017). Bankinfosecurity.com. Retrieved 9 May 2017, from http://www.bankinfosecurity.com/social-security-tries-two-factor-authentication-again-a-9900

About GAVS

GAVS Technologies (GAVS) is a global IT services & solutions provider enabling digital transformation through automation-led IT infrastructure solutions. Our offerings are powered by Smart Machines, DevOps & Predictive Analytics and aligned to improve user experience by 10X and reduce resource utilization by 40%.

For more information on how GAVS can help solve your business problems, write to inquiry@gavstech.com
www.gavstech.com

GAVS