CASE STUDY

HEALTHCARE

Kings View Behavioral Health Systems

Central California mental health organization seeks clarity on their wireless security vulnerabilities.

KINGS VIEW
Behaviorial Health Systems

A leader in behavioral health, Kings View has been serving the underserved since 1951. With a strong tradition of commitment, their focus is on serving rural communities where other health resources are often limited. Treating people with care and compassion is the cornerstone of their philosophy.

Services Delivered

- ✓ Access Point Impersonation
- ✓ Encryption Review
- ✓ Spectrum Analysis
- ✓ Wireless Vulnerability Assessment

> *We engaged Breadcrumb Cybersecurity to perform an on-site wireless security assessment for all twelve of our locations throughout California. Their local presence and deep understanding of the medical industry make them an ideal choice for our organization.*

- **Gretta** Petersen
Director of Operations Support Services
Kings View

Objective

Having a dozen mental health facilities located throughout California, the Kings View corporate compliance team required clarity as to the security vulnerabilities on their wireless networks. 'Could our medical devices be hacked?' 'Is our patient data vulnerable?' 'Is our security sufficient to detect and stop attempted breaches?' The selected security partner not only had to provide clarity on these vulnerabilities, but ensure that recommendations furthered the organizations HIPAA compliance goal.

Solution

When approaching the Kings View engagement, Breadcrumb engineers understood firsthand that wireless, just isn't wireless. Deficiencies within the wireless protocol, and the decentralization of wireless management, make organizational wireless networks very susceptible to unauthorized access. Leveraging their expertise within the medical community, Breadcrumb performed LIVE, onsite testing at each of the twelve locations. Real-world assessment strategies included access point impersonation, discovery and exploitation of hidden networks, interception of wireless data and the review of encryption protocols. Customer wireless devices (medical devices, iPad's, laptops, etc.) were also targeted during the assessment, evaluating their relative strength and resistance to a sustained attack. Lastly, complex mathematical scenarios were used to challenge the strength of encrypted wireless passwords, producing over 200 billion attempts in the Breadcrumb lab.

Results

Having thoroughly evaluated discovered wireless networks, Breadcrumb engineers were able to deliver a comprehensive and detailed analysis of the organizations wireless security posture. Referencing a series of industry standards, and established best practices within medical environments, Breadcrumb produced actionable reporting, with prioritized recommendations. Kings View Director of Operations, Gretta Peterson noted, 'We were very pleased with the results of Breadcrumb's engagement and found their recommendations invaluable.'

Breadcrumb™
CYBERSECURITY

☎ 559.578.4800 | *breadcrumbcyber.com*

| Evidence is Everywhere

Copyright © Breadcrumb Cybersecurity 2019 All Rights Reserved.