CASE STUDY

EDUCATION

Clovis Unified School District

Prominent California school district engages Breadcrumb Cybersecurity to assess public facing IT infrastructure.

CLOVIS UNIFIED SCHOOL DISTRICT

Honored more than 100 times as California Distinguished Schools, Clovis Unified serves nearly 43,000 students. The district has thirty-three elementary schools, five intermediate schools, five high schools, four alternative schools, one adult school, one online school, and one outdoor and environmental education school.

Services Delivered

- ✔ External Black Box Assessment
- ✔ Physical Control Review
- ✔ Targeted Social Engineering
- ✔ Web Application Assessment
- ✔ Wireless Assessment

> *"The team at Breadcrumb definitely understands security and how to demonstrate cyber risk. They're a great resource to organizations like ours."*
>
> - **Raj** Nagra
> *Chief Technology Officer*
> Clovis Unified School District

Objective

While internal security risks are more readily understood by organizations, external exposures are far more challenging to define and protect against. The exploitation of data leveraged from publicly available sources is often the cornerstone of destructive cyber-attacks. Serving a population of nearly 43,000 students, Clovis Unified School District sought to more clearly understand its external security posture and vulnerabilities, with the ultimate goal of better protecting its sensitive data assets.

Solution

Targeted cyber-attacks are extremely challenging to predict, let alone prevent. When a hacker has selected a target for breach, it's generally a matter of time before they are successful. The key to disrupting this process is better understanding your organization through the eyes of a hacker. Assuming the role of a determined threat, Breadcrumb engineers conducted a 'no-knowledge' black box assessment. Over the course of eight (8) weeks, Breadcrumb methodically assessed the public facing IT assets of CUSD, systematically evaluating them for security vulnerabilities. Utilizing discovered data, Breadcrumb engineers built a comprehensive 'breach profile,' highlighting areas of increased breach probability. In addition, Breadcrumb engineers conducted an onsite security assessment of district wireless (Wi-Fi) assets and physical access controls. Various strategies and tactics were used to carefully, and responsibly conduct all onsite evaluations. Concluding the engagement, Breadcrumb developed custom social engineering campaigns, demonstrating the impact of targeted cyber-attacks.

Results

Having carefully worked through the engagement process, Breadcrumb engineers produced real-world outcomes, demonstrating the impact of targeted attack scenarios. Leveraging Breadcrumb's results, Clovis Unified moved forward with confidence in better understanding their risks and how to mitigate them.

Breadcrumb™ CYBERSECURITY
559.578.4800 | breadcrumbcyber.com