nexdigm

Case Study

A Food Processing Enterprise

Service(s) offered: **Cyber Resiliency (Virtual CISO Office)**

Sector/Industry: **Food Processing**

Augmenting IT and compliance protocols for a Food Processing enterprise across multiple locations

The client (Client) is a leading food processing and poultry farming enterprise. With several state-of-the-art research facilities and farms, they are committed to offering products that are healthy for consumption and sustainable to the environment.

Challenge

- The Client worked on an inefficient network infrastructure which hindered future business growth plans.
- The Client's geographical presence spanned 450 locations across India.
- The Client uses a specialized patented formula which needed to be kept secure. Hence, it was important to create and implement a customized IT infrastructure that could protect and prevent possible breaches.
- The Client needed a trusted partner to help enhance their cyber security infrastructure, aligned to industry best practices/frameworks.
- As the business grew inorganically, the underlying technology platform was built in bits and pieces. Hence, there was an absence of a governance structure for the platform which led to ineffective cyber resiliency.

Case Highlights

- Nexdigm's in-depth Vulnerability Assessment and Penetration Testing (VAPT) highlighted several risks which were mitigated
- We discovered 17 Critical, 9 High, 9 Medium, 29 Low priority vulnerabilities as well as 13 Informative vulnerabilities
- The scope of VAPT was spread across 450 locations, 2500 nodes and 16 servers
- The Client noted 42 different observation reports in the previous year consisting of system anomalies which were rectified

- As there were multiple vulnerabilities, a holistic review and analysis of key IT infrastructure was required which involved assessing:
  - Applications
  - Network Architecture
  - Operating Systems
  - Data Storage and Transfer
- The Client also wanted to inculcate a capacity-building program that educated employees about the responsible uses of IT tools and systems to build a robust infrastructure.

Augmenting IT and compliance protocols for a Food Processing enterprise across multiple locations

Solution

The Nexdigm team assisted the Client in analyzing their existing cyber security infrastructure and the key risk areas to understand areas of improvement within the current IT infrastructure. We analyzed the current network structure through a combination of data flow schematics and industry-standard checklists to identify gaps across locations. Suitable recommendations were provided to the Client based on industry best practices to ensure risk mitigation across the entire organization.

To standardize reporting and inculcate a robust reporting mechanism, we created an inventory template report and implemented the same across all locations in India. Comprehensive monthly and quarterly dashboards were sent to the Client's management team to provide an overview of all ongoing tasks.

Our ethical hacking team conducted a vulnerability assessment of four crucial applications being used across their pan-India locations and identified serious gaps and loopholes which exposed the organization to multiple breaches and cyber threats.

Once the assessments and verifications were completed, we provided a roadmap that included a review and implementation plan for an entire year for IT governance as well as regulatory and other compliances. The organization is currently mitigating these gaps basis our assessment and analyses.

To ensure the Client's associates were well-versed with the industry-best practices, we also provided cyber security awareness training on:

- Network Infrastructure
- Communications Protocols
- Applications
- Database Optimization Management
- Hacking as a Service (Black / Grey Box)
- Server Security Management Reviews

We partnered with the Client to support and drive a cyber security awareness program that covered 60% of its workforce across 450 locations.

Impact

The final solution offered to the Client's management encompassed an end-to-end IT and operational solution that covered all the Client's requirements. Nexdigm introduced additional solutions to the Client as a value-added proposition which included:

- Improved information security and business continuity management
- Improved stakeholder confidence in information security arrangements
- Improved company credentials with the correct security controls in place
- Faster recovery times in the event of a breach
- Rationalized the investment in technology by 20%
- Effective roll-out of cyber security baseline that helped minimize threat exposures
- Designed a governance structure for managing its cyber resiliency
- Program aligned to its business growth strategy
- Achieved zero phishing attacks throughout the duration of the pandemic
- Created and implemented a robust IT security infrastructure for the entire organization.

Our ethical hacking team conducted a vulnerability assessment of four crucial applications being used across their pan-India locations and identified serious gaps and loopholes which exposed the organization to multiple breaches and cyber threats.

For more information on this case study, please write to us at:

ThinkNext@nexdigm.com

You can also visit our website to know how our services resulted in tangible business benefits:

www.nexdigm.com