DRAGONCY

The sharp eye of cybersec

Success Stories:
The Case for a Healthcare Medical Center

Overview

An important Medical Center based in Mexico City was very worried about phishing and ransomware incidents. They needed to urgently find a solution within their constrained budgets and resources.

Problem

Enterprise ransomware infections usually start with a malicious email and an unsuspecting user who opens an attachment or clicks on a URL of a website that is malicious or has been compromised. This is how the infection is originated. Moreover, some ransomware variants, like **WannaCry** and **PETYA**, take advantage of the fact that there are un-patched internal servers and workstations, like the windows XP embedded systems that our customer had as medical devices and end-points.

As it happens with all hospitals, its IT department was more focused on technical support to its internal medical areas and lacked focus on cybersecurity. Although they were conscious about the risks associated with WannaCry and the ransomware threats, they could not find a convincing, effective and acceptable mitigation strategy for the WannaCry, PETYA and all the emerging cyberthreats that are constantly looming.

They knew they needed to do something quickly because they were using unpatched windows XP as embedded systems all through their medical tomography, imageology, x-rays and other medical devices. Time was running against them.

Solution

Our team carefully analyzed the case and implemented our "**Assume Breach**" methodology: **Prevent, Detect and Respond**.

For this, we first prepared an email, cloud-based gateway solution that didn't demand much from the internal IT team. This is what we call a first-line of defense. At the same time, we implemented a mitigation strategy for critical systems that included isolation and traffic segregation, patching operating systems whenever possible, as well as the improvement of their threat detection process and backup and recovery strategy.

This left our customer in a solid position to contain a possible infection. As a matter of fact, we continue to support the incident response process as an on-going managed service.

Outcome

As of this day, we continue to help them mature their cybersecurity operations. They have found the right balance between smart cybersecurity investments and creating a safer digital working environment.

Although they have suffered a couple of minor incidents, we have been able to respond and recover quickly with no serious or permanent damages.

We are also mutually collaborating in the preparation of a security governance program that includes an extensive cybersecurity awareness training for its users.

709 Bryson Way, Southalke, TX 76092 (214) 284 7039 www.DRAGONCY.com