Point-of-Sale Still Not Getting the Point of Security

25
JUL

Point-of-Sale Still Not Getting the Point of Security

July 25, 2014 / Ryan Nolette / Advanced Threat Protection, Community Perspectives, Prevention

While reading through my backlog of RSS feeds recently, I came across a few articles about point-of-sale (POS) devices and their security issues. One article was on Dark Reading and another was on threat post.

The threat post article calls for POS dealers to have a sit-down and implement better security in their devices to help secure the smaller companies that are unable to afford third-party security products and services.

The Dark Reading article is about how Payment Card Industry Data Security Standard (PCI DSS) does not protect against RAM-scraping malware (the type that hit retailers like Target and Michael's).

The core of the issue in the threat post article all comes down to smaller companies waiting on their POS

dealers to secure their POS systems.

Why wait?

Let's be honest with our expectations here. Very few large companies are known for quick action when it comes to enhancing the security of their products. Why not use something to lock down the device from the start? Something like Bit9 running in high enforcement would only allow the applications you want to run on the POS system to run on it.

This is a similar issue to the one described in the Dark Reading article. These customers are dependent on their POS dealers to provide solutions for them to protect themselves.

Why wait?

RAM scrapers currently require a file artifact, which means there is a binary running on the system. With Bit9, if these are unapproved/unknown files, then they simply will not run in a lockdown environment.

So why is this even still an issue?

Most POS systems run an older version of Windows (XP, stripped down XP, or sometimes Unix). This means that these systems are vulnerable to the same issues as other Windows deployments. Common issues such as viruses, outdated third-party software (like the remote management applications their dealers require them to have installed for support and management), vulnerabilities, and poor patching cycles (some companies don't even know they need to be patched) are rampant in POS deployments. But what I find worst of all, is poor visibility at the system level.

If you run a POS system in your enterprise, do you know what is running on it? Can you stop processes that you don't know or want from running? Do you have a patching schedule? Does your POS system even have the necessary hardware requirements needed for something as bloated as modern AV POS solutions to run on it?

POS is currently considered a set it and forget it deployment. This simply isn't true.

If this is the case in your deployment, and if you aren't going to run any additional software on the system besides what comes installed by default, lock it down.

What do I mean lock it down? Remove the ability to install any other software on the system, remove the ability to run unknown and unapproved processes on the system, and run a security product so lightweight on the system that the hardware will barely notice how secure it has become.

Point-of-sales needs to better understand the point of security.