

A study of the use of IPS in a healthcare environment

Introduction

The disruption of access to IT systems in a healthcare environment can have a catastrophic impact on patient care.

This project investigates intrusion prevention systems before deploying one in a live environment to measure its security effect

Project objectives

To research the types of IDPS, their characteristics and where they are best deployed before deploying one in a live environment and measuring the effects.

Research focus

There are many types of IDPS, so these were analysed to decide which IDPS type was best to test.

All have their own positives and negatives, but a host-based intrusion detection/prevention system (HIDPS) was chosen to test as Cwm Taf Morgannwg Health Board were keen to improve the protection of their server estate, particularly for out of support operating systems

Design and testing

A HIDPS was installed on to chosen servers within the live server environment at Cwm Taf Morgannwg Health Board before vulnerability scans were run to test the IDPS's ability to identify and protect against threats

Results

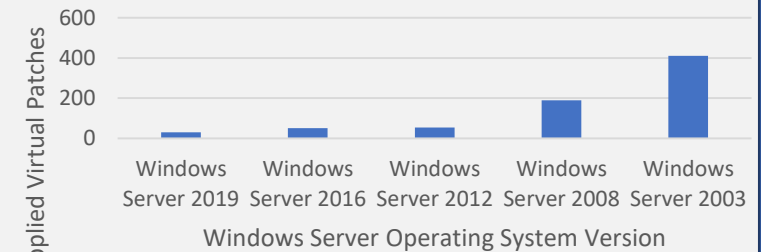
The time to patch for newly disclosed vulnerabilities dropped markedly after the installation of the IDPS. Previously, patching a newly disclosed vulnerability could take a month:

- *9 days average for patch to be created*
- *14-21 days to test patch, arrange server downtime, patch server and reboot*

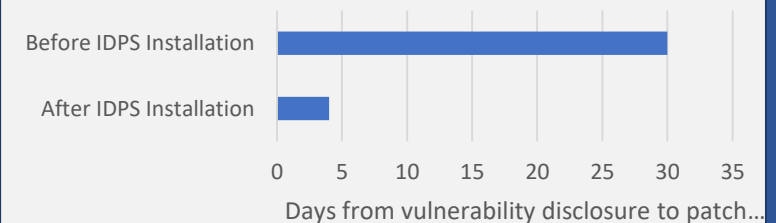
With IDPS installed, virtual patches for vulnerabilities not discovered by TrendMicro stood at 4 days. For vulnerabilities discovered by TrendMicro themselves, systems were often protected before exploits were even developed.

Legacy OS were also protected against newly discovered vulnerabilities. Server operating systems such as Windows Server 2003 were protected against roughly 380 vulnerabilities than prior to IDPS installation

Number of Additional Vulnerabilities Protected Against by Server Operating System



Time to Patch New Vulnerability



Conclusion

The project was a success. The IDPS installation proved a marked increase in the security posture of the CTM environment. So much so, that the product was purchased to cover the entirety of the CTM server estate. The IDPS is now live across all CTM servers