Organización
Ur&Penn

País:
Suecia

Solución
Panda Adaptive Defense 360 + Panda Patch Management

Licencias
250

"PAD360 ofrece una protección extremadamente buena. Hasta el momento no hemos tenido problemas de malware ni incidencias con los programas. Nada. El módulo de Gestión de Parches refuerza la seguridad de nuestras aplicaciones y actualiza su funcionalidad. Es sencillo, y funciona como un reloj."

Situación

La empresa Ur&Penn cuenta con 121 tiendas y un plan a largo plazo para la apertura de otros 80 establecimientos en Suecia. De sus actuales tiendas, 9 están situadas en Finlandia. Las 158 cajas registradoras que la empresa tiene repartidas en Suecia y Finlandia se encuentran a distintas distancias de la oficina central ubicada en Upplands Väsby, en la zona norte de Estocolmo.

Este ambicioso plan de crecimiento requiere de la máxima automatización posible de su parque informático, y para ello, Ur&Penn necesita que las soluciones seleccionadas puedan incorporarse fácilmente a cada nueva tienda abierta.

Un entorno distribuido formado por una red de tiendas ubicadas en Suecia y Finlandia requiere de un plan para poder funcionar de la mejor forma posible. Dicho plan es responsabilidad de Emir Saffar, Director de IT de Ur&Penn desde el año 2012.

La caja registradora de cada tienda es en realidad un ordenador desde el que los empleados pueden navegar, recibir correo, y leer documentos además de lo más importante: atender a sus clientes y gestionar sus pagos. Cualquier tiempo de inactividad del servicio se traduce en una interrupción completa de las operaciones diarias de venta de artículos de joyería y otros accesorios a los clientes, pudiendo generar grandes pérdidas de ingresos.

Ningún empleado ha dado muestras de cometer errores de tipo informático de forma deliberada. Sin embargo, teniendo en cuenta que tanto la navegación en Internet, como la gestión del correo electrónico y el uso de aplicaciones son una fuente posible de ataques, resulta necesario optimizar la seguridad informática.

Reto

Los equipos no actualizados (en el caso de Ur&Penn, sus cajas registradoras) son un objetivo fácil de hackers maliciosos y constituyen por tanto un grave riesgo de seguridad.

Hoy en día, el 99,96% de las vulnerabilidades presentes en los equipos de las organizaciones están relacionadas con la ausencia de determinados parches. Este es un problema global que no afecta solo a Ur&Penn. Un error comúnmente extendido es creer que tanto Microsoft/Windows como otros programas se actualizan automáticamente. Sin embargo, raras veces lo hacen.

Emir Saffar se dio cuenta de que, para poder trabajar con sus distintas tiendas, era necesario poder parchear todas ellas de forma eficaz, remota y ahorrando la mayor cantidad de tiempo posible. Así, tras muchos años con Windows Update, que obligaba a apagar los equipos y que hacía que algunos de ellos no recibiesen parches críticos de seguridad, decidió buscar una solución.

Sin una herramienta de gestión de parches resultaba difícil realizar un seguimiento de qué equipos recibían ciertos parches y en qué momento. Además, el hecho de que la responsabilidad recayese a veces en los empleados podía traducirse en equipos no actualizados (al cerrar los avisos de programas sin actualizar). Por otra parte, la necesidad de reiniciar las máquinas, un requisito de ciertas actualizaciones, podía dar lugar, como se ha explicado anteriormente, a pérdidas directas de ingresos en caso de producirse durante el horario de atención al público.

Solución

La empresa probó un gran número de soluciones de gestión de parches, muchas de ellas con opciones muy avanzadas de configuración. Además, como Ur&Penn tenía Panda Adaptive Defense 360 instalado en su red, Emir contactó también con Benny Jonasson, su comercial de Panda en Suecia. Benny respondió que Ur&Penn podía convertirse en el primer cliente sueco en probar el último módulo incluido en Adaptive Defense: Gestión de Parches.

Nada más activar el módulo (sin necesidad de instalaciones adicionales ya que Panda Adaptive Defense se encontraba desplegado en su red), Saffar pudo ver la gran cantidad de parches que no tenían instalados. Además, el módulo ofrecía una clasificación de la importancia de los parches de aplicaciones de terceros: “críticos”, “importantes” y “necesarios”, lo que permitía definir prioridades a la hora de su aplicación.

Una de las ventajas del módulo es que soporta todo el software más habitual, lo que cubre todas las necesidades de la organización, que no emplea software propio.

Panda Patch Management permite organizar los parches y programar su instalación cuando las tiendas de Ur&Penn están cerradas, evitando así molestar a los usuarios. El control es exhaustivo y contribuye a lograr un entorno mucho más seguro. La visibilidad es total: tanto de toda la actividad como de los parches que no se han podido instalar. La solución es sencilla, pero muy estable, lo que dificulta cometer errores.

En palabras de Saffar: “PAD360 ofrece una protección extremadamente buena. Hasta el momento no hemos tenido problemas de malware ni incidencias con los programas. Nada. El módulo de Gestión de Parches

refuerza la seguridad de nuestras aplicaciones y actualiza su funcionalidad. Es sencillo, pero funciona como un reloj."

Evaluación

Los informes sobre los programas, equipos y servicios parcheados y actualizados son fáciles de obtener. En resumen, Saffar es de la opinión de que el servicio es muy sencillo de utilizar y cumple su cometido a la perfección.

Principales Beneficios

Panda Patch Management permite en una única solución:

Auditar, monitorizar y priorizar las actualizaciones de los sistemas operativos y aplicaciones.

Un panel único en la consola centraliza, actualizado en tiempo real, permite una visibilidad agregada del estado de los parches y actualizaciones pendientes del sistema y cientos de aplicaciones de terceros.

Prevenir incidentes, reduciendo sistemáticamente la superficie de ataque por vulnerabilidades.

La gestión de parches y actualizaciones con herramientas de gestión, fáciles e intuitivas, permiten adelantarse a la explotación de vulnerabilidades.

Contener y mitigar ataques que explotan vulnerabilidades.

Aplicando inmediatamente las actualizaciones críticas desde la consola Cloud. La consola correlaciona detecciones con vulnerabilidades, minimizando así el tiempo de respuesta, contención y remediación mediante la actualización necesaria desde la consola. Adicionalmente, permite aislar de la red los equipos afectados, mitigando así la expansión al ataque.

Reducir los costes operativos.

- No requiere ni despliegues ni actualizaciones de agente en los endpoints, simplificando la gestión son sobrecargar los equipos y servidores.

- Minimiza el esfuerzo de las actualizaciones remotas desde la consola Cloud. Además, la aplicación de parches está optimizada para minimizar errores.

- Visibilidad inmediata y desatendida de las vulnerabilidades, actualizaciones y aplicaciones en EoL3, tras la activación.

Cumplir con el principio de responsabilidad activa.

Requisito en muchas regulaciones (GDPR, HIPAA y PCI), que obliga a las organizaciones a establecer todas las medidas que garanticen la protección de datos sensibles bajo su responsabilidad.