Organization
Ur&Penn

Country:
Sweden

Solution
Panda Adaptive Defense 360 + Panda Patch Management

Licenses
250

"PAD360 is an extremely good protection. So far, we have had no problem with either malware or incidents in the programs. Nothing has happened. With the Patch Management module, the security of the applications is further tightened and the functionality up to date; it is simple but works like a clock."

Situation

Ur&Penn has 121 stores with a long-term plan to open up an additional 80 stores around Sweden. Of the existing ones 9 are located in Finland. All of the 158 cashiers that the business in Sweden and Finland consists of, are at different distances from the head quarters in Upplands Väsby in the northern Stockholm area.

With this ambitious plan of growth, as much as possible of the IT environment is needed to be automated and there are great advantages for Ur&Penn if the IT solutions that are chosen can easily be added to each new store that opens up.

A distributed environment with the network of stores around Sweden and Finland requires a plan to be operated in the best way. This plan is made by Emir Saffar. He has been IT manager at Ur&Penn since 2012.

The cash register in each store is a computer. On that computer the employees can surf, receive e-mail, read documents apart from the most important: help customers and manage the payment. Any downtime means that the daily operations of selling jewelry and other accessories to the customers completely cease, which ultimately leads to large losses of income.

No employees have shown signs of making errors in the IT environment deliberately, but since surfing, e-mail management and application usage are possible sources for attacks, IT security needs to be optimized.

Problem

Computers (in Ur & Penns case cash registers) that are unpatched constitute a significantly easy target for malicious hackers and are thus a major security risk.

Today, 99.96% of active vulnerabilities for endpoints in organizations are related to missing patches. This applies generally and not just to Ur & Penn. One common misconception is that Microsoft / Windows and other programs stay updated automatically. They rarely do.

Emir Saffar had realized that in order to operate the various stores, they needed to be able to patch all stores in an efficient, remote and thus time-saving manner. After many years with Windows Update, where computers had to be shut down and some did not receive critical security patches, they looked for a solution.

Without a tool for patch management, it was difficult to keep track of which computers received which patches and when the responsibility was sometimes on the employees it could also mean that in addition to being unpatched (closing the warnings of unpatched programs), they could also need to restart their machines since that is required when certain updates are made and, as mentioned earlier, in Ur & Penns's case, this means direct loss of income when this was happening during regular opening hours.

Solution

Many solutions for patch management were tested, several with the possibility of very advanced settings. Since Ur&Penn already had Panda Adaptive Defense 360 installed, Emir also contacted Benny Jonasson, his sales contact at Panda in Sweden. Benny replied that Ur&Penn could be the first customer in Sweden to test the latest module for Adaptive Defense; Patch Management.

When this module was applied (without any additional installation because they had already deployed Panda Adaptive Defense), Saffar could immediately see how many patches were not yet installed. The grades on third-party patches were also displayed, in the form of "critical", "important" and "necessary". This sets priority order on what should be addressed first.

One advantage is that all "regular" software are supported, so Saffar sees no need to further have to patch, as they do not use any proprietary programs.

With Panda Patch Management, they have got the patches in order, which can be scheduled in order not to disturb at all; hence this can be done when the stores are closed. The control is comprehensive and contributes to a considerably safer environment. Everything can be seen: what happened and which patches did not succeed. The solution is simple, but very stable. This makes it difficult to make mistakes.

Saffar says: "PAD360 is an extremely good protection. So far, we have had no problem with either malware or incidents in the programs. Nothing has happened. With the Patch Management module, the security of the applications is further tightened and the functionality up to date; it is simple but works like a clock. "

Evaluation

Reports on which programs have been patched and which computers and services have been patched and updated are easy to take out. In summary, Saffar is of the opinion that it is a very simple service, which fully fulfills its function.

Main use:

Panda Patch Management allows, within a single user-friendly solution:

Audit, monitor and prioritize operating systems and application updates.

The single-panel view offers centralized up-to-the-minute and aggregated visibility into the security status of the organization with regard to vulnerabilities, patches and pending updates of the systems and hundreds of applications.

Prevent incidents, systematically reducing the attack surface created by software vulnerabilities.

Handling patches and updates with easy-to-use, real-time management tools that enable organizations to get ahead of vulnerability exploitation attacks.

Contain and mitigate vulnerability exploitation attacks with immediate updates.

Panda Adaptive Defense 360 console, in conjunction with Patch Management, allows organizations to correlate detected threats and exploits with the uncovered vulnerabilities. Response time is minimized, containing and remediating attacks by pushing out patches immediately from the web console. Additionally, affected computers can be isolated from the rest of the network, preventing the attack from spreading.

Reduce operating costs.

- Panda Patch Management does not require the deployment or update of any new or existing endpoint agents, simplifying management and avoiding workstation and server overloads.

- Minimizes patching efforts as updates are launched remotely from the cloud-based console. Additionally, installation is optimized to minimize errors.

- Provides complete, unattended visibility into all vulnerabilities, pending updates and EOL3 applications immediately after activation.

Comply with the accountability principle contemplated in many regulations (GDPR, HIPAA and PCI). It forces organizations to take the appropriate technical and organizational measures to ensure proper protection of the sensitive data under their control.