Managing My Company's Security is a Nightmare Says Panda Security Director

Wednesday 15 May, 2013

Opinion article/byline by Luis Corrons, Technical Director of PandaLabs, Panda Security

If you are a head of corporate security I am sure the words above will have run through your mind more than once. The majority of top-level executives are focused on targeted attacks (by far the most heavily covered malware stories, just take a look at the latest Twitter, Facebook, Apple or Microsoft attacks, for example), however heads of corporate security know better than anybody else what risks they are facing and what their priorities are:

- Neutralize attacks before they impact corporate productivity.
- Prevent data theft.

A major hurdle to achieving these two 'simple' objectives stems from evolutions in the way we interact with IT such as BYOD ("Bring Your Own Device") and cloud computing. Both of these have brought about important changes in the way data is managed. IT Departments are very often one step behind users, and unfortunately in most cases there is no real control over all devices on the corporate network. Additionally, cloud storage applications allow users to store all kinds of data in the cloud without any real control from the IT Department, with all the inherent security issues involved.

Despite perimeter solutions still being a necessity, the corporate perimeter must now expand to include new devices (mainly smartphones and tablets) that also handle confidential corporate information. Also, it is worth remembering that these devices can become an entry point for intruders into the corporate network, so it will be necessary to control the devices as well as the information.

Add to this the fact that most infections and attacks take advantage of un-patched vulnerabilities that exploit security flaws for which there are security updates available, and you realize patch management along with applications that enable full control and visibility of the network status are essential for organizations.

These needs cannot be satisfied by so called 'traditional' antivirus software, instead other, more advanced solutions are required. The latest trend in the computer security industry is that of Endpoint Protection Platforms, which provide a collection of security utilities including: hardware and software audits, patch and vulnerability management, application control, etc. Traditional antivirus software is still necessary but not sufficient.

For heads of corporate security it is also very important that the network monitoring tool doesn't require new servers, VPN connections, etc. In this context, simple solutions where administrators install a lightweight agent on every managed device, allowing control regardless of whether they are in the office or on the road though a Web browser, are gaining ground spectacularly. Mobility presents new challenges in IT risk management and troubleshooting, and the ability to access devices remotely will help organizations reduce costs and boost their productivity significantly.

Luis Corrons, Technical Director of PandaLabs, Panda Security

Visit the PandaLabs blog at http://pandalabs.pandasecurity.com/

Media:



Related Sectors:

Business & Finance :: Consumer Technology ::

Related Keywords:

Anti Virus :: Malware :: Panda Security ::

Scan Me:

Company Contact:

_

Panda Security

T. 08443353791
E. neil.martin@uk.pandasecurity.com
W. https://www.pandasecurity.com/uk/

View Online

Additional Assets:

Newsroom: Visit our Newsroom for all the latest stories:
https://www.pandasecurity.pressat.co.uk