Building A Secure Manufacturing Infrastructure

Grant McDonald, Product Marketing Manager for Symantec SMB & .cloud

Today’s manufacturing is a wonder of efficiency and cost-effectiveness. However, the same technology that makes it possible for smaller manufacturers to thrive in our global economy also presents security challenges. The digital design process makes it easier than ever for employees to share information with one another and outside experts, but at the same time, with every endpoint connected to the Internet, there is always a risk of a cybercriminal stealing this intellectual property or other sensitive information.

As we develop more ways to collaborate and share information, criminals are also working on new ways to steal it. Information is the new currency among thieves, and the right individuals will pay top dollar for a competitive advantage, whether through outright theft or by disabling critical systems. One of the main attack points for cybercriminals today is the endpoint, which can be compromised in a variety of ways. Malicious emails are always waiting for employees to click on them, and these days it is easier than ever to use publicly available information to create sophisticated false messages to trick users into disclosing their credentials. Malware can also find its way onto user machines via USB devices and even through visiting well-known websites that have been infected. Hackers can also gain access to endpoints by exploiting weaknesses in network defenses.

Smaller manufacturers may have assumed themselves immune from attacks on their SCADA systems, because of their proprietary nature. But recent incidents such as Stuxnet have revealed that there is no limit to the lengths cybercriminals will go. Malware like Stuxnet also shows that even physical machinery is no longer safe from threats. This vulnerability is likely to be further highlighted as technology continues to evolve and sophisticated IT components take a more active role in the manufacturing process.

Today’s smaller manufacturers should implement a multi-layered approach to security, with a focus on not only protecting their physical equipment, but also their information — which can make up 40 percent of an SMBs’ business value, according to the *Symantec 2012 State of Information Survey*. In order to accomplish this, they need to combine effective policies and user precautions with robust security technology.

The Human Element

One of the most effective methods for protecting endpoints is to educate users on the threat landscape. Most users are aware that spam emails can contain malicious links, but many of them are unfamiliar with today’s phishing techniques that involve more personalized messages. So, it’s important to give employees regular reminders of endpoint safety techniques. One of the most important areas to emphasize is the potential dangers of social networking sites (including accepting requests from unknown people). It’s also important to establish policies concerning where sensitive information can be stored, and monitoring employees to ensure compliance.

Security Technology

Most businesses, regardless of size or industry, are using multiple security solutions. Aside from creating unneeded complexity within an IT system, it can also create unnecessary costs. Smaller manufacturers are placing information in more places than ever before — desktops, servers, cloud and virtual services, plus mobile devices. And servers are especially important endpoints to protect, because not only are they vital to maintain the availability of both applications and information, but they are also where two-thirds of data breaches happen.

One of the most effective ways to secure resources is to simplify the number of solutions wherever possible, deploying more comprehensive, complementary tools that provides overlapping protection.

Today’s security tools also go beyond traditional definition-based malware recognition, which is critical given the constant emergence of never-before-seen threats. Smaller manufacturers should guard against these through reputation-based security, which takes advantage of intelligence gathered from millions of other machines to maintain real-time protection.

For those looking to upgrade or consolidate their endpoint security solutions, they should consider whether on-site security software will best meet their needs, or whether a cloud-based solution would be a better option. The advantage of a managed service is that protection is always up to date, and security status information is typically available from any Internet connection. It is also available as a managed service, reducing the time needed to maintain protection and automatically handling issues that come up.

Manufacturing is undergoing a revolution as outdated systems are replaced with integrated technologies that more efficiently coordinate activities. But at the same time, today's businesses need to be aware that threats are evolving quickly as well. Endpoints are often at the front lines of the cyber security battle, and as information is being stored and accessed in more places than ever before, manufacturers need to make sure they deploy strong endpoint protection as an important part of an overall security plan.

Grant McDonald is a Senior Global Product Marketing Manager at Symantec focused on endpoint protection for small and mid-sized businesses. He has over 15 years of experience in IT and marketing across a variety of technologies and industries and he is a passionate cloud enablement evangelist for businesses of all sizes and industries. Learn more at www.symantec.com *[1].*

Links:
[1] http://www.symantec.com/small-business/