Highlights from a recent webcast on Automating Client Health

SECURITY CONFIGURATION MANAGEMENT BEST PRACTICES

Ami Casto of Adaptiva, and Dale Meredith, Pluralsight author, trainer and consultant, discussed problems and solutions for security configuration management in a recent webcast.

It's not good to have your systems shut down by ransomware.

It's even worse, if you discover that the malware that broke into your system would have been stopped if you'd applied the patch from your operating system vendor that you'd been putting off doing for weeks or months.

"Too busy to patch" doesn't sound like a good excuse after an attack.

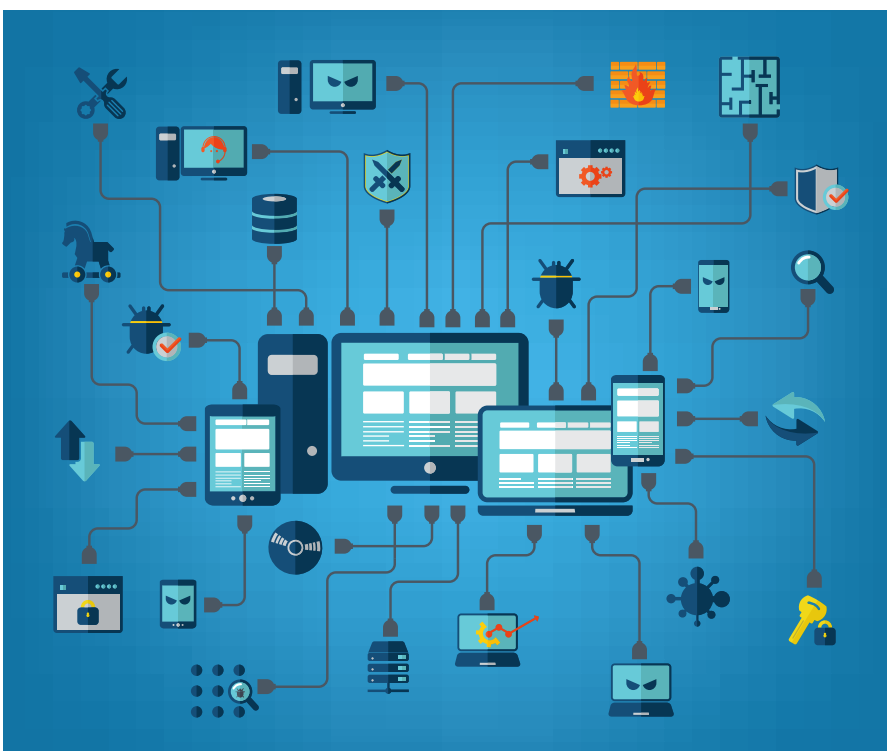
But there is some truth in that it's hard to get around to doing routine patches when you're spending the day putting out fires for your end users and working on rush projects.

Many IT professionals are in this bind.

But the ones who found a way to make the necessary patches even with their hectic schedules are glad they did.

Don't Postpone Patching

Dale Meredith, Pluralsight author, trainer and consultant, said this was true of the recent wannacry ransomware attack.



MaDeDee / Shutterstock.com

"What we discovered with this particular piece of ransomware is that it could have been avoided, and in fact a lot of companies avoided it simply by doing patches and updates," he said.

If you have a choice, you want to be in the shoes of those who avoided disaster by simply doing updates and patches.

Ami Casto of Adaptiva understands what harried IT professionals are facing as both technology and business objectives change with lightning speed.

"It's difficult to fix issues across an entire environment, day in and day out and still focus on moving the business and its technology forward," she said. "Whether it's a company of just a few people to several thousand people, admins themselves don't have the time or energy to track and remediate rogue assets."

Casto pointed to an Information Age survey that shows 44 percent of the time system administrators spend day in and day out is on troubleshooting and administrative tasks. This includes having to manually track down, remediate, document, close tickets. The survey also found that 32 percent of IT decision makers are spending time reacting or bracing for issues, whether it's an internal breach or bracing for or recovering from an audit. The answer, she said, is automated security configuration.

> "It's difficult to fix issues across an entire environment, day in and day out and still focus on moving the business and its technology forward."—*Ami Casto of Adaptiva*

Automating Security Configuration

"Without an automated security configuration, no one's able to move forward," Casto said. "All of the resources are chasing ghosts and wasting energy being reactive rather than proactive."

She listed a dizzying short list of questions from everyone from end users to CxOs that IT pros, whether IT administrators or IT decision makers, have to answer:

Are the employee's operating systems configured correctly? Is it the correct version of Windows 10, Windows 7 even 8.1? Is it setup to defer feature updates but still allow security updates? Are all the endpoints receiving the latest patches? What about the ConfigManager client? Is it installed and working correctly? If you are using the ConfigManager to manage and maintain your environment and actually deliver those patches, is the client okay? Can it reach the management point? Is there something wrong with the infrastructure? Are the right security settings supplied?

"What you really see is that there becomes a need to have a more adaptive security configuration," Casto said. "What you set up in the beginning has to adapt to your needs as the business grows, or as needs change or as audits change."

Adaptiva, founded with a vision to deliver cost-effective ways for enterprises to scale their IT initiatives by intelligently doing more with the resources they already own, offers a solution.

"We've developed a great suite of products that have been well tested and adapted by large organizations that have a lot of issues and they don't have a lot of staff or time to go after the little nagging things that tend to eventually bring down an organization," Casto said.

Client Health

One of the key Adaptiva products is Client Health, an endpoint security configuration engine.

"What this means is that you can design a custom security check and remediation action that you can give to a computer, or a group of computers to run," Casto explained. "That can identify issues such as, there's something wrong with the config manager agent. There's nothing worse than being on the help desk and an end user reports an issue that could have be resolved had the config manager client itself worked."

Client Health helps avoid annoying problems for end users and systems administrators alike. It can make sure nothing is blocking software updates, so they are not left spinning on the software catalog. It can identify and fix common roadblocks to updates including clearing the software distribution folder or ensuring there is enough disk space.

"Now you can have something that's proactively looking for these things going wrong and automatically detecting and automatically repairing and automatically reporting back to you," Casto said. "We have 75 built-in checks across a vast number of categories. Security would be of the most interest today. It checks things like is my PowerShell execution policy matching what was dictated by my security requirements? Is my config manager client actually healthy? Is the installation media actually healthy and available for everyone that's targeted to have this config manager client?

With the proliferation of tablets and smart phones in the workplace, manual configuration of all those endpoints becomes problematic and costly.

"It does cost a lot of money to manually troubleshoot," Casto noted. "That's when you start to see high turnover in your helpdesk staff because they are getting burned out doing silly tasks that should actually be automated and should have a bit of intelligence to them."

Adaptiva Client Health offers the fastest and most automated way to manage endpoint health including:

- Drive endpoint compliance and configurations at scale
- Create endpoint health checks instantly without coding
- Increase endpoint management efficiency with intelligent automation