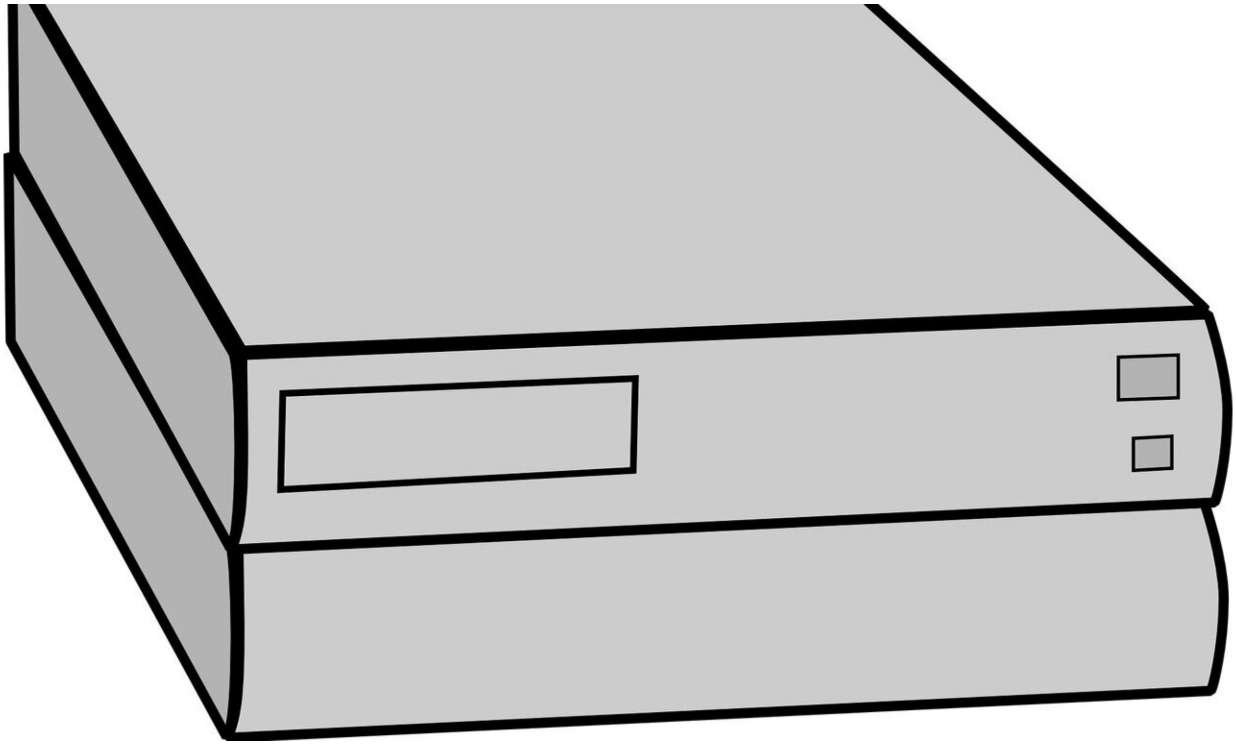
As more work from home, Dell unveils new BIOS shield

April 15 2020, by Peter Grad



Credit: CC0 Public Domain

As millions of employees are suddenly working from home, computer security threats are on the rise. The sudden rush to set up home offices means many users working on insufficiently protected devices are exposing businesses to unprecedented new exposure to malicious hackers.

"While the world is grinding to a halt, cyber-attacks are on the rise, preying on public fear and anxiety," says Yenni Tim, researcher of Cybersecurity at the University of New South Wales Business School in Sydney, Australia.

In an effort to combat security threats, Dell Technologies last week released a utility that will protect one of the most sensitive components of a computer, the BIOS. Frequently the target of the most malicious malware assaults, the BIOS oversees critical computer processes, from boot-up to system configuration parameters.

A compromised home computer poses serious risk of stolen identity, passwords, fiscal data and personal information. But when home computers are connected to corporate accounts, the risk is immensely compounded.

It is not the element of working from home that is the problem, but the sudden surge in the number of systems that must be monitored, said David Konetski, a Dell vice president.

"Previously, for many companies, only a fraction of their workforce was working remotely full time," Konetski explained. "When most companies' security systems and processes were originally put in place, they were created to scale, but not at the rapid rate we're experiencing today."

Dell's new utility, named the Dell SafeBIOS Events and Indicators of Attack, relies on behavior-based threat detection to spot imminent assaults and alert IT teams. It provides visual analysis of BIOS alterations before and during threats.

When a threat is detected, system administrators can isolate the targeted device and employ remediation strategies.

Dell is also providing other security tools to business customers. They include VMware Carbon Black for advanced threat detection and vulnerability management; Secureworks' vulnerability assessment, detection and response tools; and extended licenses for Dell Encryption services.

Dell SafeBIOS Events and Indicators of Attack is available for download at the Dell web site.

The crush of millions of new users working from home has brought out the worst in some malicious actors in the digital world. But there may be an upside as well. Companies worldwide are reevaluating their notions of office work. Many are reimbursing employees for costs associated with setting up home offices, including furniture and computer equipment.

With such changes in perceptions about remote work and increasing fiscal allocations to achieve it, some companies may rethink a new post-COVID-19 work-from-home environment.

"This is not how I envisioned the distributed work revolution taking hold," Matt Mullenweg, chief executive of the popular web site host WordPress, told The Guardian recently. Mullenweg, who also heads Automattic, owner of Tumblr, already widely deploys remote workers. He said the current crisis "might offer an opportunity for many companies to finally build a culture that allows long-overdue work flexibility."

"Millions of people will get the chance to experience days without long commutes, or the harsh inflexibility of not being able to stay close to home when a family member is sick," Mullenweg said. "This might be a chance for a great reset in terms of how we work."

More information: blog.dellemc.com/en-us/dell-te … days-remote-workers/

Citation: As more work from home, Dell unveils new BIOS shield (2020, April 15) retrieved 25 April 2024 from https://techxplore.com/news/2020-04-home-dell-unveils-bios-shield.html