Digital Security
Progress. Protected.

Protecting SMBs with multiple layers of defense

As Russia's attacks on Ukraine continue, you may wonder: Will Russia launch cyberattacks against the US? Who could be affected? Should I be worried? How can I protect my business?

These questions are justified as the conflict prompted a series of alerts from government agencies and cybersecurity organizations. Back in March 2022, the White House issued a Statement by President Biden on our Nation's Cybersecurity, warning about the potential of malicious cyberactivity by Russia against the United States in response to the economic sanctions imposed by western governments.

Although the advice is especially targeted at organizations and businesses that fall into the critical infrastructure category, where a disruption can potentially cause chaos (as witnessed in the case of Colonial Pipeline,) all businesses should take heed and prepare accordingly.

If you're a small business and believe you're not in danger because you're not as interesting to bad actors as large enterprises, consider the following statistics. According to the Identity Theft Resource Center's 2022 Business Aftermath Report, more than 45% of small businesses surveyed lost revenue due to cybercrime.

In addition, 50% of SMBs in the survey reported losing control of a social media account to a cybercriminal, with 87% of the victims losing revenue generated by the account.

Just like large enterprises, small businesses handle sensitive data and can become collateral damage from attacks aimed at other targets. Small businesses can also be seen as stepping-stones to attack large enterprises or critical infrastructure business partners. Indeed, no company is too small to be noticed by criminals—which is why it's probably time for you to re-evaluate your current cyber solutions.

Having set the scene with the need for preparedness, what technologies and actions should cybersecurity admins at small businesses consider? First, see this article from WeLiveSecurity regarding cyber resilience and the US's Cybersecurity and Infrastructure Security Agency (CISA) Shields Up campaign. The advice mentions ESET Dynamic Threat Defense, now known as ESET LiveGuard Advanced, a technology designed to

detect zero-day exploits, which should be a priority given that the conflict in Ukraine is ongoing.

ESET LiveGuard Advanced can detect new and previously unknown threats by running them in a cloud sandbox. Detecting threats the first time they are encountered can sometimes demand more processing power and memory than is readily available on employees' machines. ESET LiveGuard offloads the task of detecting such threats to more powerful machines in the cloud. Once these samples are in the cloud sandbox, they can be subjected to multiple machine learning models and robust detection techniques to classify them as clean, suspicious, or malicious. It's a zero-day game changer.

Another area of focus should be the reduction of the attack surface to minimize the risk of a bad actor gaining access to your network and identifying a zero-day vulnerability to be exploited either now or in the future.

Employee devices typically account for a significant portion of the attack surface, and with hybrid workforces being the new norm, revisiting the policies and technology used to protect endpoint devices will assist with reducing risk. To address the heightened need to protect corporate endpoints with multiple layers of defense, a combined package of protection, such as ESET PROTECT Complete or ESET PROTECT Advanced, is recommended.

Next: See our Zero-Days Resource Guide

Get started: Talk with one of our experts

eset Digital Security
Progress. Protected.