Two basic actions that reduce enterprise cyber risk by 60% - Infosec Resources

Drew Robb

5-7 minutes

Earlier this year, intelligence reports related to events in Ukraine indicated an upsurge in Russian cyberattacks. As a result, U.S. President Joe Biden issued a warning and requested that organizations be more vigilant and do all they can to thwart Russian cyber-actions.

“This is a critical moment to accelerate our work to improve domestic cybersecurity and bolster our national resilience. I have previously warned about the potential that Russia could conduct malicious cyber activity against the United States, including as a response to the unprecedented economic costs we’ve imposed on Russia alongside our allies and partners. It’s part of Russia’s playbook. Today, my administration is reiterating those warnings based on evolving intelligence that the Russian government is exploring options for potential cyberattacks,” said President Biden.

Before the announcement, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) issued a Shields Up alert that included mitigation guidance for anyone suffering an attack.

“The federal government can’t defend against this threat alone,” said the president. “Most of America’s critical infrastructure is owned and operated by the private sector, and critical infrastructure owners and operators must accelerate efforts to lock their digital doors. If you have not already done so, I urge our private sector partners to harden your cyber defenses immediately by implementing the best practices we have developed together over the last year.”

The warning followed a series of recent incidents in the U.S. and Europe. The FBI announced, for example, that a ransomware gang had breached the networks of more than 50 U.S. infrastructure organizations, including energy, nuclear, water, and manufacturing facilities. In addition, more than 20 American companies working in liquefied natural gas (LNG) production suffered cyberattacks, including Chevron and Cheniere Energy. Around the same time, hackers disrupted vital oil terminals at ports in Europe. And in 2021, Colonial Pipeline was locked out of its systems by ransomware, sending gas prices soaring.

The basics: Passwords and patch management

Some may listen to such news and dire warnings and panic. But fear and panic only worsen the situation. Those who keep their own houses in order by following the basics are likely to avoid serious mishaps during these times.

According to the Incident Response Analytics Report from Kaspersky, two key actions address most cyber incidents. Stronger password policies combined with patch management can reduce the risk of cyber incidents on business by as much as 60%. Unfortunately, both are weak points in many organizations.

According to the report, “Security issues with passwords and unpatched software combine into the overwhelming majority of initial access vectors during attacks.”

Researchers also noted that a brute-force attack is by far the most common method hackers use to invade an enterprise. This tactic throws raw processing power at passwords to break them. It is often successful if relatively weak passwords are in place. “123456” and “administrator” passwords may seem comical examples, yet they are still found by hackers attempting to crack passwords. But many other easily cracked examples, such as names and dates of birth, can be breached by brute-force approaches. Strong passwords combined with multi-factor authentication (MFA) are recommended.

The report also noted that 31.5% of successful attacks take advantage of known exploits. Much of the time, the vulnerabilities utilized by adversaries are several months old. Quite a few are greater than one year old. One has even passed its tenth anniversary, yet it is still unpatched in some enterprises. Comprehensive patch management, therefore, decreases the risk of a security incident by more than 30%.

Securing systems with the basics

In light of this data, the report summarized the key actions enterprises need to take to secure their systems:

- **Implement robust password policies** supported by MFA, along with identity and access management. Over the past two years, password standards have moved from six to eight and now ten or more characters, including a symbol, capital letter and number (or a long, easy-to-remember password phrase). Users may grumble, but this is necessary to prevent brute-force success.
- **Implement patch management** to take care of OS and application updates and known vulnerabilities. Automated patch management suites can help organizations deploy patches rapidly, prioritize them based on security ratings and take the drudgery out of this function.
- **Conduct comprehensive and effective third-party** security awareness training programs for employees. Phishing remains an effective tactic for cybercriminals. User education is a must to lower the incidence of users clicking on links and malicious attachments.
- **Implement** endpoint detection and response **solutions** to detect and react to attacks promptly.

With nation-state cyberattacks ramping up, it’s important to shore up your organization’s cybersecurity basics. Make sure you’re not missing the low-hanging fruit before focusing on more advanced security measures.

Sources

- Statement by President Biden on our Nation’s Cybersecurity, The White House
- Incident response analyst report, Kaspersky

Reprinted from: https://resources.infosecinstitute.com/topic/two-basic-actions-reduce-enterprise-risk/