Protect Your Organization From Cyber and Ransomware Attacks

Security

February 14, 2018

Contributor: Laurence Goasduff

Patching and removing web server vulnerabilities will improve enterprise security through 2021.

Alison, chief information security officer at a London hospital, is not having a bad dream. This morning, she received a notification that ransomware has affected a large proportion of the IT systems across the organization. The immediate impact is a major interruption in the hospital's ability to provide services to patients, affecting appointments, patient history records and communications. The potential longer-term effects are the loss of personal data that could be both sensitive and critical to patient care.

Ransomware families have grown by more than 700% since 2016

This scenario is a reality for many IT leaders. It is not just something that happens to someone else; it is happening to both small and large organizations, indiscriminately, across all industries globally. Malware, and more specifically ransomware, are a real and significant threat, driven by the rise in criminal cyber skills and the ease with which such campaigns generate money. Malwarebytes found that ransomware families have grown by more than 700% since 2016, and Datto asserts that as many as 35% of attacks are resolved through paid ransoms.

Originally, tackling the malware problem was far simpler. Individual exploits were matched with a single vulnerability, which gave rise to signature-based technologies such as antivirus software.

Threat analysis isn't about the threats themselves. It's about the organization's specific vulnerabilities and the exposure of those vulnerabilities.

During the past few years, threats have significantly evolved. This means the regular release of custom malware that is able to address multiple, distinctive attacks based on the same vulnerability, which makes the threats far harder to identify and deal with using traditional signature-based technologies. CIOs and security and risk management leaders now find themselves grappling with how best to protect their organizations against these different classes and variants of attack.

IT

Build resilience in a world of escalating risk

Ahead of the Gartner Identity & Access Management Summit 2018, Gartner research director Pete Shoard warns these leaders that simply counting the number of attacks is fruitless.

“They need to realize that threat analysis isn’t about the threats themselves; it’s about the organization’s specific vulnerabilities and the exposure of those vulnerabilities,” says Shoard. “It’s also a combination of security technology engagement, understanding where the crown jewels are stored, and how the business pursues new digital business initiatives.”

Below, Shoard shares some tips on the most effective safeguards, from patching and vulnerability management to securing web applications and web servers.

Protect your organization

- **Carry out regular vulnerability scanning** to provide visibility of potential risk exposure to your organization, enabling prioritization of key issues.
- **Concentrate on basic functions**, such as patch-oriented security practices and system hardening.
- **Disable nonessential and unused services** in order to prevent the spread of malware within corporate networks.
- **Educate end users** on why and how to remain vigilant when opening attachments or clicking on links from senders they do not know.
- **Install the latest updates** for operating systems and security toolsets; vendors react quickly to high-profile threats so expect such updates to be released out of sync with the expected schedules.

- **Back up copies of your files** and have them stored elsewhere. Cloud-based services are often unaffected by such incidents, but local and network copies of files are likely to be at risk.
- **Restrict user and local accounts** from having administration access, where possible, and implement privileged access management solutions where appropriate.

Respond to threats: Key recommendations

The protection gap is widening as the monetary gains from threats such as ransomware become more attractive to cyber criminals. Furthermore, the spread of encryption that blinds network security has been responsible for the lack of visibility in detection technologies. Both these trends have led to greater burdens on enterprise security and the ability to sustainably tackle vulnerabilities.

Key recommendations for CIOs and security and risk management leaders:

- Use the latest endpoint and network detection technologies, which have inbuilt prevention and response capabilities, to enable your teams to react faster to the threats affecting your organization. It is also critical that you have effective remediation and response plans to allow your teams to continue operating when the worst happens.
- Secure your web applications and web servers, and consider using web application firewalls. Through 2021, Gartner estimates that the second most impactful enterprise activity to improve security will be removing web server vulnerabilities.
- Do not underestimate the need to gain better visibility of, and to better secure, shadow IT. Gartner estimates that by 2020, one-third of successful attacks experienced by enterprises will be on data located in shadow IT resources, including shadow Internet of Things. Carrying out regular security assessments to gain better visibility or implementing zero-trust networking can be an effective way to tackle such threats.