Lodestone

Hardening the Frontlines of Ransomware Defense

It's possible to spot intruders and eject them from the premises, but it's faster, safer and less expensive to stop them at the front gate.

With robust internal controls, organizations can identify breaches more quickly and prevent malicious actors from moving around and accessing data in any systems they do penetrate.

Human beings are almost always the weakest link in an IT security system. A mass phishing attack can be directed at hundreds or even thousands of a company's employees.

THREE INFECTION POINTS REPRESENT A LARGE SHARE OF BREACHES TODAY

1. Ransomware threat groups take advantage of vulnerabilities in common network services and in internal systems. Well-known recent attacks through these gaps include EternalBlue, WannaCry and BlueKeep. Today's improved firewalls and authentication tools can help prevent a bad actor from penetrating a network but still allow legitimate users to get in the front door.

2. Human beings are almost always the weakest link in an IT security system. Most people create their own passwords and some reuse them across platforms, making them more widely available to thieves and easier to crack. Even passwords that are difficult to guess can be stolen from databases and other sources.

3. A mass phishing attack can be directed at hundreds or even thousands of a company's employees. If even one person takes the bait and clicks on a link, attackers can bypass firewalls, compromise systems and steal data.

ORGANIZATIONS CAN TAKE ACTION IN THREE MAIN AREAS TO PREVENT INTRUSIONS

A combination of technical improvements and changes in users' behavior can beef up barriers to intruders. Hardening the external attack surface is relatively straightforward, new tools and best practices can help make remote access more secure, and awareness training can help users recognize risks and prevent breaches.

HARDENING THE EXTERNAL ATTACK SURFACE

In addition to patch management and other routine maintenance, organizations can use hardening mechanisms to mitigate specific attack vectors, protect especially

vulnerable parts of the surface and reduce overall risk. New vulnerabilities in software are known as “0 days” due to their release being before vendors have developed a fix, but most attacks based on these vulnerabilities are directed at the highest-value targets such the military, government agencies and the largest financial institutions.

Many companies isolate systems that need external access from more valuable internal systems and data through the use of a “demilitarized zone” or DMZ, and layers of firewalls. Systems like web servers which need to be accessed by users externally can be placed in a DMZ and heavily restricted and monitored while still being connected to the greater organization for easier management.

We urge organizations to regularly scan externally facing infrastructure for potential vulnerabilities. Penetration tests, for example, are “mile wide, inch deep” looks at networks. These tests can be mostly automated and relatively inexpensive. Experienced analysts can mount deeper, more tailored and hands-on tests to find vulnerabilities in specific portions of a network.

We urge organizations to regularly scan externally facing infrastructure for potential vulnerabilities.

SECURING REMOTE ACCESS

Organizations of all kinds are now relying more on secure remote solutions, such as multi-factor authentication (MFA), which add layers of authentication mechanisms to prevent stolen credentials from leading to a successful system compromise. Each approach has strengths and weaknesses—usually trade-offs among security, usability, administration overhead and financial cost.

For most organizations today, best practices include using MFA in combination with a virtual private network (VPN) solution to provide secure, encrypted access to internal systems from remote external locations. Navigating this world can be complex, however. Microsoft’s Remote Desktop Gateway (RDG) is not a VPN but it does funnel remote desktop protocol (RDP) over secure channels and supports MFA. RDG can reduce the potential attack surface by providing a single point of secure external connection. Due to the complexity of proper, secure RDG configuration and the frequency of vulnerabilities identified with the RDP protocol, we recommend that RDGs be implemented behind VPNs, both with MFA enabled.

RAISING SECURITY AWARENESS

As threats evolve, employees and other systems users need consistent training—an annual phishing test will accomplish very little and only highlight the risks that can be posed by a single careless or distracted employee.

We recommend constant testing and mandatory refresher training. Begin with training users how to look for clues—systems administrators can even identify themselves in the first mock phishing emails or messaging. As training progresses, administrators can send increasingly sophisticated and realistic phishing simulations. Many vendors and consulting firms can provide this kind of training and testing; we urge organizations to choose the approaches best suited to their needs including price, platform, content and results.

As people get training—and fair warning that they will be tested—administrators can send increasingly sophisticated and realistic phishing simulations.

Senior leaders also need to help employees understand and practice good overall operational security. Phishing is not the only form of social engineering. Other common risks include:

— Phone calls purporting to be from the help desk or support center asking for login credentials.

— Wire transfer fraud. Everyone who handles wire transfers should know what clues to look out for and how to follow up on odd requests without interrupting business flow.

— Physical risks, such as “tailgating” or “shoulder surfing.” Privacy screens can help.

— Weak and reused passwords. We recommend using a password manager and passphrases that are long but easy to remember.

Organizations facing skilled, determined or numerous attackers may benefit from subscribing to feeds or services that provide information about threat actors, ransomware campaigns and other emerging threats. Some of these services are free and included with appliances; paid services may provide fuller, up-to-date feeds.

Vendors such as haveibeenpwned.com, for example, collect caches of compromised usernames and passwords from publicized breaches and provide users with the ability to see where their credentials were exposed. While these systems can't identify every name or password that has been compromised, they do provide a shock value, which can spur users in to taking more precautions. Organizations can take additional measures to look up addresses with an application programming interface, or look up their entire domain by providing ownership of their domain record.

NEXT STEPS

IT expertise is becoming more important than ever, but each employee plays a vital role on the cybersecurity team. They all need to understand their responsibilities clearly and help defend the organization and themselves from internet-facing vulnerabilities, credential theft and social engineering. Cultural and behavioral changes are also as important as technical advances.

Unfortunately, the attackers will keep coming. We need to work together recognize and manage evolving risks, close gaps where we find them and respond quickly and decisively when breaches do occur.

ABOUT LODESTONE

Lodestone, a leader in comprehensive cyber defense, we're known for doing it differently. By blending best-in-class design, intelligent service and technology with human insight, our experts, provide clients with the information and processes needed to address cyber threats across the spectrum—from strategic readiness through digital forensics and incident response.

Josh Sudbury is the Managing Principal, Forensic Investigations. Josh Sudbury is a cybersecurity professional with over 20 years of experience in technology across multiple verticals. For the past six years, he has been consulting in the information security space, with a specialty in Digital Forensics and Incident Response (DFIR).

For more information on Lodestone, visit: Lodestone.com or contact us at info@lodestone.com

www.lodestone.com
320 E. Main Street
Lewisville, TX 75057