Courtesy of
MST Insurance Solutions, Inc.

CYBERRISKS&LIABILITIES_

Lateral Movement in Cyberattacks

Cybercriminals employ several tactics to steal as much data as possible during a cyberattack. One such tactic is the lateral movement technique. After breaching an organization's network, attackers navigate across systems to infiltrate additional devices and access more sensitive information. This technique allows them to expand the depth and impact of an intrusion.

To reduce the risk of lateral movement, business leaders should ensure their organizations have robust cyber defenses and well-developed incident response protocols. These measures help safeguard networks and contain threats before attackers can access more critical systems.

This article explores why cybercriminals utilize lateral movement, explains how it works and discusses techniques malicious actors may use to execute it. It also offers actionable strategies businesses can implement to prevent it from occurring.

How Lateral Movement Works

Lateral movement within a network starts when cybercriminals conduct external reconnaissance concerning their targets. In this phase, the malicious actors gather information about the potential victim's data, network, devices, systems and users. Various technologies help them obtain information, allowing them to identify objectives, note potential vulnerabilities and select entry points.

After the cybercriminals have collected sufficient information, they move on to the next phase, known as the initial breach. This occurs when a cybercriminal evades endpoint security through various tactics, including phishing schemes, credential stuffing, or installing malware to steal or compromise login passwords. Then, the attacker can access a secured network while appearing to be a legitimate user.

After entering the network, the cyberattackers can expand their foothold within it and access other systems and devices. They may also establish backdoor entry points to allow them to reenter the network undetected, if a security response removes them. These backdoors often take the form of hidden user accounts, rogue scheduled tasks or modified remote access settings that persist even after apparent cleanup efforts. In some cases, attackers may also deploy additional malware or scripts to automate their lateral movement and maintain control.

The intruders then capture assets and accounts with higher privileges, making it harder for them to be removed from the system. This privilege escalation can culminate when hackers secure administrative privileges, allowing them to move practically unencumbered through the network and access sensitive data. Finally, malicious actors may delete logs, modify time stamps or take other actions to remove traces of their intrusion and make detection even more difficult. By the time defenders detect unusual activity, the attackers may have already exfiltrated data, deployed ransomware or established long-term surveillance within the network.

Why Do Cybercriminals Use Lateral Movement Techniques?

There are several reasons why cybercriminals may utilize lateral movement while carrying out their attacks, but one of the main reasons is that it allows them to more easily evade detection by cyber defense systems. This is because their movement within the network appears legitimate due to their use of stolen credentials. This freedom of movement also provides access to a wider range of sensitive data.

This Cyber Risks & Liabilities document is not intended to be exhaustive nor should any discussion or opinions be construed as legal advice. Readers should contact legal counsel or an insurance professional for appropriate advice.

Another reason this tactic may appeal to hackers is that they can discover system vulnerabilities while they are inside a network and use that knowledge to escalate their attacks. Their stolen credentials allow them to conduct this reconnaissance over a long period, permitting them to identify weak points they can exploit while minimizing the likelihood of detection and removal.

Techniques Used in Lateral Movement

Specific techniques hackers may utilize to move laterally within a system include the following:

- **Internal spear-phishing**—This is where the intruder targets specific groups or people within the organization by sending them an email with a malicious attachment or link from a previously compromised internal account that appears trustworthy.
- **Remote services exploitation**—These are attacks where a cybercriminal gains access to a company's remote services (e.g., Remote Desktop Protocol, virtual private networks or collaboration platforms like Microsoft Teams) and uses them as a starting point to move further into the network or access confidential systems and data.
- **Pass-the-hash attacks**—These occur when cybercriminals obtain a system's password hash (a mathematical representation of a password) and use it to authenticate without needing to know the original password, allowing them to impersonate legitimate users.
- **Pass-the-ticket attacks**—These involve hackers stealing Kerberos authentication tickets (used in many Windows environments) to impersonate users and access services across the network.

Preventing Lateral Movement

There are several techniques cybercriminals use to carry out a cyberattack with lateral movement, and their methods are constantly evolving. However, businesses can take action to reduce the likelihood of these cyber incidents occurring. Strategies to consider include:

- **Implement network segmentation**. By dividing a network into isolated segments, an organization can control the traffic that flows through the segments and more readily limit the movement capabilities of an intruder.
- **Use "least-privilege" and "zero-trust" principles**. With the principle of least privilege, users only have access to resources needed to complete their job tasks. This can limit hackers' movement capabilities if the legitimate user's password is compromised. Additionally, applying zero-trust principles, where no user or device is trusted by default and every access attempt must be verified, can significantly reduce the risk of lateral movement.
- **Leverage technology**. Technological solutions, including artificial intelligence and machine learning, can help businesses detect anomalous activity within a network and can help stop an attack before it escalates. Endpoint detection and response tools, antivirus software, regular security patches and firewalls should also be utilized.
- **Consider managed detection and response systems**. These services utilize a combination of advanced technology and human expertise to provide around-the-clock monitoring of an organization's network. They can help detect and respond to cyberthreats in real time, including those involved in lateral movement.
- **Practice good cyber hygiene**. Proper cyber hygiene can help prevent hackers from stealing passwords or other security tokens that can allow them to infiltrate a device or network. Passwords should not be stored in plain text, and password hashes should be kept in secure, encrypted areas. Regularly updating software, disabling unused accounts and monitoring for unusual activity are also key practices.
- **Require multifactor authentication (MFA)**. Requiring users to identify themselves through more than one verification factor can add a critical layer of protection. Even if a password is stolen, MFA makes it significantly more difficult for attackers to gain unauthorized access, thereby limiting the chance for lateral movement within the network.
- **Bolster protection of administrative accounts**. Extra precautions should be put in place for users

with administrative privileges. For example, administrators should have a separate account for day-to-day business (e.g., emailing and web browsing) and a privileged account that is used only for administrative functions. This can help reduce the chances of an infected device being used to access an administrative account.

- **Deploy honeypots**. Honeypots are decoys set up to attract malicious actors while not exposing legitimate systems or infrastructure. If a honeypot is accessed, it may indicate that an intruder is attempting to perform lateral movement or scan the network. Such activity should trigger an investigation and response.

Conclusion

Lateral movement within a network can significantly worsen a security breach, placing large amounts of sensitive data at risk. To address this exposure and protect an organization’s critical assets, implementing strong cybersecurity practices is essential. By being proactive, businesses can mitigate this risk, detect threats earlier and shield their operations from the costly consequences of cyberattacks.

Contact us today for more information.