TOP 3 WAYS TO IDENTIFY A VULNERABLE VENDOR

To protect against cyberthreats and data breaches, IT organizations deploy a range of protocols and security solutions for their internal users. But given that 61% of data breaches in the U.S. are attributed to a vendor or third party, it’s clear that IT departments need to focus their security on vendor remote access.

Without control over third parties, how can you ensure they have the right security in place to prevent an attack from infiltrating your system? Even if you don’t have visibility into third-party networks, here are some red flags to help you determine if a vendor may be vulnerable or compromised.

1. **Have they been hacked before?**

   The best indicator of a future breach could be a past breach. Companies who have had a breach before are more likely to experience a breach again. Look for signs to include:
   - They either deny or get defensive if a past breach is brought up.
   - They are unable to provide documentation on how they fixed the issue that led to the breach.
   - They don’t have a plan to prevent similar attacks from happening in the future.

   **What to do if you see these red flags**

   Research vendors to see if they have a history of breaches before going into contract. Industry-specific sites are a good resource. For instance, the US Health and Human Services office maintains a database of reported breaches in the healthcare industry. Knowing the history of breaches can inform your vendor interviews and clarify how they’ve changed their security approach to prevent future issues.

2. **Do you see unusual vendor activity on your network?**

   Audit your vendor’s activity. Keep granular logs to flag irregular behavior that might include a hacker attempting to launch ransomware or another attack. Look for signs to include:
   - Unusual login hours for vendors
   - Odd source of IP addresses or domains
   - Unusual or unapproved server access
   - Large file transfers

   **What to do if you see these red flags**

   First, determine if the behavior is truly suspicious. Perhaps an employee accessed files on Saturday night to prepare for a Monday meeting. Even if the activity does not indicate a problem, it could be a security threat to your data — and potentially your business’s revenue and reputation — at risk. You may wish to put additional controls on that vendor going forward, including limiting file transfers such as time or duration limitations, or approvals required for access.

3. **Do you have general concerns about the vendor’s security practices (or lack thereof)?**

   Maybe you have concerns about a vendor but can’t quite prove it. Some of the top indicators that your vendor could be compromised include:
   - The number of users and/or sessions is higher than in previous days/weeks/months.
   - Your vendor demands you use a remote access tool you don’t feel comfortable with and wants direct access to your systems.
   - Your vendor requests “always-on” access to critical systems.
   - Your vendor asks for a shared credential and cannot demonstrate good privileged access management practices for handling the credential, such as vaulting and obfuscation.
   - Your vendor requests “always-on” access to critical systems.

   **What to do if you see these red flags**

   SecureLink can help strengthen your authentication practices such as multi-factor authentication, awareness programs, and understanding cloud and on-premises environments. You may also consider hiring an outside vendor to take a deeper look to ensure a breach hasn’t occurred from the vendor.

About SecureLink

SecureLink is a leader in managing secure vendor privileged access and access support for both highly regulated enterprises and technology vendors. We are trusted by organizations to protect privileged access across multiple industries as health care, finance, technology, government, education, and retail. SecureLink’s secure, purpose-built platform protects your organization’s digital assets and data. SecureLink is headquartered in Austin, Texas. Go to securelink.com/demov to call us at 888.897.4498.