How vulnerable is your network to a third-party data breach?

Protecting your network is about more than a mix of cybersecurity solutions. It's about creating a culture of awareness. Hackers are always looking for an easy target. If you don't regularly assess your security protocols and demand high standards of your privileged partners, you may find yourself making headlines for a very costly breach.

There's too much at stake to allow gaps in your third-party vendor security. A breach puts everything at risk- from business continuity and reputation, to customer relations and compliance standings.

Take a 360-degree view of your vendor access management habits, systems, and tools before hackers set their sights on your network. It will probably be eye-opening to discover your potential exposure.

THE WEAKEST LINKS

The most common ways hackers exploit third-party access

Hackers look for the path of least resistance to access a target. Nearly half of the time, it's through a third-party vendor. It's important to understand the frequently exploited vulnerabilities of third-party remote access to keep your company, and your network, safe.

These best practices make it more difficult for hackers to access your network via a third-party vendor. Reference the checklists below to see how you can, and should, be monitoring different aspects of your cybersecurity strategy.

Virtual Private Networks (VPN)

A popular tool to provide remote access, this solution makes it difficult to set and restrict granular access privileges. To use a VPN properly, and in the most secure way, make sure you:

- Reserve privileged VPN credentials for internal employees.
- Limit vendor access to only the applications and systems they need to get their jobs done.
- Implement monitoring and activity audit capabilities to ensure users are acting within their permissions.

Phishing

Social engineering uses the "desire to help" mentality of your team against you and the security of your network. If employees expect bad actors, they will become more aware of the possibility and will, in turn, also become less of a liability. To ensure your company is prepared for any phishing attack, make sure you:

- Establish mandatory vendor training and testing with the latest phishing schemes.

Malware and Ransomware

Hackers often use phishing techniques to deploy these types of attacks. Include the following to keep your data safe:

- Team training should cover prevention, containment, and all necessary cybersecurity awareness trainings.
- Ensure that all security patches are updated.

Privileged Credentials

A vendor's compromised credentials could put an entire network at risk. In fact, 80% of hacking-related breaches leverage privileged credentials. To combat hacking-related breaches:

- Implement multi-factor authentication that's tied to the vendors' company systems.
- Store credentials in a repository so only authorized users can gain access with temporary, permission-based access, all without ever seeing app-level credentials.

Is your vendor a target?

Tell-tale signs of low-hanging fruit

Vendors might provide niche services at a fair price, but all of the advantages of using a vendor might be wiped out if you're not on the same page when it comes to cybersecurity.

Assess the security policies and practices of your vendors - because you are only as secure as your most vulnerable partner.

Have you identified any of these red flags that would make your vendor prone to a cyberattack?

- The vendor's security practices and policies are poorly defined.
  - Insist the partnership depends on them taking the necessary steps for alignment.
- No third-party security audit or industry certifications such as SOC or ISO.
- They have already had a security breach.
  - If a vendor has had one security breach, another is likely.
  - Be concerned if they are unable to provide documentation of steps taken to address the vulnerability.
- No ability or history of internal security audits.
- The vendor requests for carte blanche access to critical systems and does not offer a robust security action plan.
  - Provide only the minimum access needed for the vendor to do their job and make sure to also conduct frequent spot audits.

How transparent is your network activity?

Clarity is power

Tracking employee usage can be fairly straightforward.

It's more challenging to monitor and control vendor activity, but critically important to the security of your network.

How well do you know what's happening on your network? Take the guesswork out by:

- Implementing multi-factor authentication to ensure only authorized users get access.
- Getting real-time alerts with every vendor users' connection and disconnection.
- Tracking and recording all network activity.
  - Get granular details for every user session– who was on, what systems they accessed, and what they did down to the keystroke.
- Requiring vendors to provide documentation of cybersecurity training, policies, and their own internal audits of which files or servers they've accessed.
- Conducting your own spot audits and annual due diligence of vendor activity to track unusual traffic patterns.

What are your privileged access management standards?

Maintain control and least privilege

Remember, it's estimated that 80% of hacking-related security breaches are related to privileged credentials. So, while vendors might request an "all-access" approach, your company is in the driver's seat regarding who receives privileged access.

Take a least privileged approach when dealing with partners that need remote access – and ensure you always have the option to kick users off at any time.

Are you giving away too much access to vendors and putting your company at risk? These are must-have policies and solutions:

- Not all vendor reps require privileged credentials.
  - Develop a policy that stipulates the critical circumstances under which these credentials are granted to vendors.
- Consider using a Vendor Privileged Access Management (VPAM) platform that gives vendors access only to the systems they need for their work.
  - A centralized solution will provide more control and visibility to limit vulnerabilities.
- Protect against compromised credentials.
  - Eliminate the threat of shared credentials with multi-factor authentication and ensure that vendor reps have their own, individual accounts.
  - Store privileged vendor credentials in a secure vault and ensure every login is tied to an individual, not just an account.
- In the event of a data breach, reduce the time to identify the breach, the impact, and resolve it by:
  - Installing suspicious activity alerts.
  - Capturing comprehensive user activity records.
  - Implementing firewalls and segmented user stations, which can provide additional layers of protection.

Ensure your network isn't vulnerable to a third-party data breach

If you're only as strong as your weakest vendor, don't have a weak vendor. Or, better yet, have a system in place that keeps you protected from external threats associated with third-party remote access, like a vendor privileged access management platform. **To learn more, contact SecureLink today.**

RELATED CONTENT

THE IMPORTANCE OF A VENDOR ACCESS MANAGEMENT PLATFORM

More often than not, your company's cybersecurity policy revolves heavily on internal employees, their access, and the rules around what's okay and what isn't. But, what about your external employees – like your vendors, third parties, and contractors? Usually, these external entities are able to access important and confidential information. In order for your company's cybersecurity strategy to be well-rounded, it should include a vendor access management platform.

VIEW eBOOK

securelink.com | 888.897.4466 | contact@securelink.com