Best Practices for Vendor Access Management

Third-party vendors are a key part of the enterprise supply chain. From accounting to data analytics, they are the invisible deft hand that keeps your company running smoothly. But your most trusted business relationship may also be your Achilles' heel when it comes to security. In June, payment details for millions of Ticketmaster customers were hacked through one of the company's third-party vendors.

But the popular ticket retailer isn't the only one vulnerable to an attack. Vendors are well-known for having less-than-robust security protocols; a glaring vulnerability that makes them prime targets for hackers looking for a backdoor into company networks. While there's no one fix that can shield your company from an attack, following industry best practices for vendor access management can significantly reduce your level of exposure and strengthen your defenses against the next threat.

Take A Closer Look at Your Vendors

Do you know how many vendors have access to your network? If you're like most companies, the answer is probably "no". But not knowing who your vendors are and the security risk that each one poses increases the chances of your company being attacked. You can reduce this unnecessary risk by taking a closer look at your vendors and implementing the following strategies:

Create a List of all third party vendors. This list should include the most relevant and up-to-date contact information for each vendor, as well as, the type of access each has to your network. An IDC report found that 74 percent of organizations authorized vendor access to sensitive information which resulted in a major security incident or data breach.

Identify top-priority vendors. These are the vendors whose services are most critical to your day to day operations.

Determine which vendors pose the greatest security risk. Depending on the nature of your vendor relationships, the most vulnerable vendors could be those who have access to the most sensitive data, those who lack basic security protocols or both.

Request that vendors fill out a detailed questionnaire about their security procedures that includes information on:

> Vendor-specific security practices (i.e. firewalls, employee security training, penetration testing etc.)
>
> Past and or current known vulnerabilities in hardware or software

Policies concerning data breach reporting (*Does your vendor have one*?)

Curb Network Access

Once you have a clear picture of who your vendors are and their respective security vulnerabilities, you should assess whether or not each has the appropriate level of network access. Privileged Account Management (PAM) systems are great for managing employee access, but are, by themselves, unable to provide the highest level of vendor security. For that, you'll want to combine a PAM with a remote access security platform. This powerful duo allows you to curb vendor access by:

Allowing vendor access *without* network credentials. Vendors have access to what they need to "get the job done", and nothing more.

Eliminating shared account login access for vendors. The latest "Cost of a Data Breach Report" by IBM and Ponemon, found that 63 percent of confirmed data breaches could be tied to "weak, default or stolen passwords". Eliminating shared accounts, which can potentially be shared with hundreds of individuals, greatly reduces this third-party security threat. Multi-factor verification that links to a specific user's phone or business email account is best. Remember, it only takes one password written on a sticky note or computer spreadsheet for a hacker to gain access to your network.

Auditing, scheduling and recording vendor sessions. Gain real-time visibility into vendor activity including the "what/when/how" of vendor access, data on the deletion or transfer of information, recordings of end-user support and remote desktop sharing sessions, and an in-depth time-stamped account of database events, plus SSH logs.

Adjusting vendor privileged credentials as necessary. Vendors often work with transient contractors. Make the necessary access adjustments based on who is or *is not* a current employee.

Automating the entire vendor access management process. Optimize your business efficiency and improve security breach preparedness to better mitigate the effects of the next security breach.

Legally Protect Your Business

It only takes one poorly secured vendor to bring your entire organization to a screeching halt. The now infamous Target breach was the result of a vulnerability in an HVAC vendor's security protocols. More than 70 million customer records fell into the hands of hackers. You can better protect your business, legally, and significantly reduce your exposure to a third-party security breach with these basic best practices:

Ensure that your vendors have internal security controls that are in line with your own. Data and privacy regulations may be stricter than in the past, but that doesn't mean that your vendors are up-to-date on these policers or even compliant with them. Require your vendors to submit to a detailed questionnaire about regulatory compliance - so you can be certain that you're on the same page. Initial contract signing and contract renewals are the best time to obtain this information as vendors are most likely to be responsive when money is on the table.

Find out if your vendors are aware of data breach reporting regulations. The healthcare sector is a common target for hackers, who stand to make unlimited profits from healthcare fraud. Indeed, two of the biggest third-party vendor breaches of 2018 came from this sector. One vendor security breach released 270,000 patient records containing everything from demographic information to addresses and insurance identification numbers. But the most egregious error came in the vendor's violation of HIPAA's 60-day maximum timeframe for data breach reporting. While the financial penalties for such a violation may eventually be recouped, customer trust may be lost for good. Vendors need to understand the consequences of non-compliance.

The most difficult part of vendor access management is understanding that it's an ongoing process. Each time you add a new vendor, the process starts again. Audits must be ongoing, policies updated accordingly and adherence to security protocols strictly enforced. But once you've mastered these best practices and have integrated a SecureLink Enterprise solution, your vendor access management strategy should be as seamless as your vendor relationships.